BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS

-Última comunicación incorporada: "A" 6017-

Texto ordenado al 15/07/2016

B.C.R.A.	TEXTO ORDENADO DE LAS NORMAS SOBRE "REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS"

Índice

Sección 1. Aspectos generales.

1.1. Eficacia.
1.2. Eficiencia.
1.3. Confidencialidad.
1.4. Integridad.
1.5. Disponibilidad.
1.6. Cumplimiento.
1.7. Confiabilidad.

Sección 2. Organización funcional y gestión de tecnología informática y sistemas.

2.1. Comité de Tecnología Informática. Integración y funciones.
2.2. Políticas y procedimientos.
2.3. Análisis de Riesgos.
2.4. Dependencia del área de Tecnología Informática y Sistemas.
2.5. Gestión de Tecnología Informática y Sistemas.

Sección 3. Protección de activos de información.

3.1. Gestión de la seguridad.
3.2. Implementación de los controles de seguridad física aplicados a los activos de información.

Sección 4. Continuidad del procesamiento electrónico de datos.

4.1. Responsabilidades sobre la planificación de la continuidad del procesamiento de datos.
4.2. Análisis de impacto.
4.3. Instalaciones alternativas de procesamiento de datos.
4.4. Plan de continuidad del procesamiento de datos.
4.5. Mantenimiento y actualización del plan de continuidad de procesamiento de datos.
4.6. Pruebas de continuidad del procesamiento de datos.

Sección 5. Operaciones y procesamiento de datos.

5.1. Responsabilidad del área.
5.2. Inventario tecnológico.
5.3. Políticas y procedimientos para la operación de los sistemas informáticos y manejadores de datos.
5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.
5.5. Mantenimiento preventivo de los recursos tecnológicos.

Índice

5.6. Administración de las bases de datos.
5.7. Gestión de cambios al software de base.
5.8. Control de cambios a los sistemas productivos.
5.9. Mecanismos de distribución de información.
5.10. Manejo de incidentes.
5.11. Medición y planeamiento de la capacidad.
5.12. Soporte a usuarios.

Sección 6. Canales Electrónicos.

6.1. Alcance.
6.2. Procesos de referencia.
6.3. Requisitos generales.
6.4. Escenarios de Canales Electrónicos.
6.5. Matriz de Escenarios.
6.6. Glosario de términos utilizados en la Sección 6.
6.7. Tablas de requisitos técnico-operativos.

Sección 7. Delegación de actividades propias de la entidad en terceros.

7.1. Actividades Factibles de Delegación.
7.2. Responsabilidades propias de la entidad.
7.3. Formalización de la delegación.
7.4. Responsabilidades del tercero.
7.5. Implementación del procesamiento de datos en un tercero.
7.6. Control de las actividades delegadas.
7.7. Planificación de continuidad de la operatoria delegada.

Sección 8. Sistemas aplicativos de información.

8.1. Cumplimiento de requisitos normativos.
8.2. Integridad y validez de la información.
8.3. Administración y registro de las operaciones.
8.4. Sistemas de información que generan el régimen informativo a remitir y/o a disposición del Banco Central de la República Argentina.
8.5. Documentación de los sistemas de información.

Tabla de correlaciones.

El Directorio o autoridad equivalente de la entidad (Consejo de Administración, en el caso de entidades financieras cooperativas, o Funcionario de primer nivel jerárquico, en el caso de sucursales de entidades financieras extranjeras) es el responsable primario del establecimiento y la existencia de un área que gestione la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas para todos los canales electrónicos por los que las entidades financieras realizan el ofrecimiento de sus productos y servicios. Dicha área evidenciará una clara separación organizacional con relación a los sectores usuarios de la misma.

Del mismo modo, será responsable de que existan políticas generales y planes estratégicos de corto y mediano plazo, y de la asignación de los recursos necesarios para la mencionada área.

Debe estar involucrado con los aspectos generales que gobiernen la tecnología de la información y sus actividades relacionadas, los riesgos que conllevan, y evidenciar mediante documentación formal la toma de decisiones, el seguimiento y el control de lo establecido.

Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de las áreas de sistemas de información, los cuales involucran al Directorio, Consejo de Administración o autoridad equivalente, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos:

1.1. Eficacia.

La información y sus procesos relacionados, debe ser relevante y pertinente para el desarrollo de la actividad. Debe presentarse en forma correcta, coherente, completa y que pueda ser utilizada en forma oportuna.

1.2. Eficiencia.

El proceso de la información debe realizarse mediante una óptima utilización de los recursos.

1.3. Confidencialidad.

La información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.

1.4. Integridad.

Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.

1.5. Disponibilidad.

Los recursos y la información, ante su requerimiento, deben estar disponibles en tiempo y forma.

1.6. Cumplimiento.

Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades financieras.

1.7. Confiabilidad.

Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la entidad, en la presentación de informes financieros a los usuarios internos y en su entrega al Banco Central de la Republica Argentina y demás organismos reguladores.

Todos estos aspectos deben ser aplicados a cada uno de los recursos intervinientes en los procesos de tecnología informática, tales como: datos, sistemas de aplicación, tecnología, instalaciones y personas.

Las secciones siguientes de la presente norma enumeran una serie de requisitos mínimos que las entidades financieras deberán cumplir, los que serán sometidos a supervisión por parte de la Superintendencia de Entidades Financieras y Cambiarias.

2.1. Comité de Tecnología Informática. Integración y funciones.

Las entidades financieras deberán constituir un "Comité de Tecnología Informática" integrado, al menos, por un miembro del Directorio o autoridad equivalente, y el responsable máximo del área de Tecnología Informática y Sistemas.

Los directores, consejeros, y funcionarios definidos en el párrafo precedente, que integren el Comité de Tecnología Informática, asumen, respecto de sus demás pares del órgano directivo o, si correspondiera, de la autoridad máxima en el país, una responsabilidad primaria frente a eventuales incumplimientos a estas normas.

El Comité de Tecnología Informática deberá, entre otras gestiones:

- vigilar el adecuado funcionamiento del entorno de Tecnología Informática;
- contribuir a la mejora de la efectividad del mismo;
- tomar conocimiento del Plan de Tecnología Informática y Sistemas, y en caso de existir comentarios en relación con la naturaleza, alcance y oportunidad del mismo, el Comité deberá manifestarlos en reunión;
- evaluar en forma periódica el plan mencionado precedentemente y revisar su grado de cumplimiento;
- revisar los informes emitidos por las auditorías relacionados con el ambiente de Tecnología Informática y Sistemas, y velar por la ejecución, por parte de la Gerencia General, de acciones correctivas tendientes a regularizar o minimizar las debilidades observadas; y
- mantener una comunicación oportuna con los funcionarios de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, en relación con los problemas detectados en las inspecciones actuantes en la entidad y con el monitoreo de las acciones llevadas a cabo para su solución.

El Comité de Tecnología Informática deberá reunirse periódicamente a fin de llevar a cabo las tareas asignadas. La periodicidad mínima de dichas reuniones será trimestral, y en las mismas participarán, además de sus integrantes, los funcionarios que se consideren necesarios a fin de tratar un tema en particular.

A su vez, el mencionado Comité elaborará un acta en la cual se detallarán los temas tratados en cada reunión, así como los puntos que requerirán su seguimiento posterior. Dicha acta será transcripta en un libro especial habilitado a tal efecto y se enviará al Directorio, o autoridad equivalente, para su toma de conocimiento en la primera reunión posterior de dicho órgano.

2.2. Políticas y procedimientos.

El Directorio, o autoridad equivalente, debe procurar y observar la existencia de políticas y procedimientos para administrar el riesgo relacionado a los sistemas de información y la tecnología informática.

Las políticas son documentos de alto nivel, que representan la filosofía de la entidad y el pensamiento estratégico en la dirección de la misma. Para ser efectivas deben ser claramente escritas y concisas.

Los procedimientos son documentos escritos que describen de manera secuencial la forma de ejecutar una actividad para lograr un objetivo determinado, dentro de un alcance establecido. En dichos documentos se enuncian procesos operativos, se definen responsabilidades, se establecen los documentos (planillas, informes, registros) a emitir y controlar, y se detallan los controles necesarios, definiendo dónde y cuándo éstos deben realizarse.

Tanto las políticas como los procedimientos deben estar claramente escritos, formalmente comunicados, mantenerse actualizados, establecer la asignación de responsabilidades, y ser la base de la coordinación y realización de las tareas, como así también el instrumento que permita el entrenamiento sobre las actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas de la entidad.

2.3. Análisis de Riesgos.

El Directorio, o autoridad equivalente, será responsable de la existencia de mecanismos de control del grado de exposición a potenciales riesgos inherentes a los sistemas de información, de la tecnología informática y sus recursos asociados. Serán a la vez los responsables primarios de observar su continua ejecución.

Se deberá evidenciar la existencia de análisis de riesgos formalmente realizados y documentados sobre los sistemas de información, la tecnología informática y sus recursos asociados. Los mismos permanecerán disponibles para su revisión por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

Los resultados de los análisis mencionados y sus actualizaciones periódicas deben ser formalmente reportados al Directorio, o autoridad equivalente, que será el responsable primario de gestionar que las debilidades que expongan a la entidad a niveles de riesgo alto o inaceptable sean corregidas a niveles aceptables.

2.4. Dependencia del área de Tecnología Informática y Sistemas.

El área de Tecnología Informática y Sistemas -o la denominación que la entidad haya determinado usar para la función de la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas- dependerá a nivel organizacional, dentro de la estructura de la entidad financiera, de un lugar tal que no genere dependencia funcional de áreas usuarias de su gestión.

La entidad debe notificar formalmente la designación del responsable de área a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, cada vez que ocurra un cambio en la gestión.

2.5. Gestión de Tecnología Informática y Sistemas.

2.5.1. Planificación.

El Comité de Tecnología Informática y Sistemas, tendrá a su cargo asegurar que los sistemas de información y tecnologías relacionadas concuerden con las necesidades de negocio de la entidad financiera y se alineen con los planes estratégicos de la misma.

Se deberá evidenciar la existencia de un plan de tecnología y sistemas, formalizado y aprobado por el Directorio, o autoridad equivalente de la entidad, que soporte los objetivos estratégicos de la misma, contenga un cronograma de proyectos y permita demostrar el grado de avance de los mismos, la asignación de prioridades, los recursos y los sectores involucrados.

2.5.2. Control de gestión.

Se evidenciará la existencia de reportes formales, que sean el resultado del control ejercido por los sectores que dependen del área Tecnología Informática y Sistemas. Dichos reportes servirán como base para informar a instancias superiores, y deberán mantenerse, por lo menos durante 2 (dos) años, para su control por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

2.5.3. Segregación de funciones.

El área de Tecnología Informática y Sistemas deberá presentar una clara delimitación de tareas entre los sectores que estén bajo su dependencia.

El cuadro del punto 2.5.4. muestra, como referencia, las incompatibilidades existentes entre las funciones de un sector específico, con respecto a las actividades desempeñadas por otras áreas o sectores.

En el cuadro, donde se indica la intersección de dos funciones mediante la sigla “NO”, la entidad deberá tomar medidas en la segregación de tareas, a efectos de evitar su concentración.

Cuando en el cuadro se indica la intersección de dos funciones mediante la sigla “X”, esto implica que preferentemente estas tareas no deberían recaer en un mismo sector, y en el caso de que las mismas estuviesen concentradas, deberán evidenciarse claras medidas de control compensatorio.

En aquellos casos excepcionales, en que por razones de imposibilidad de estructura no pueda segregarse alguna de las funciones antes mencionadas, deberá evidenciarse la existencia formal y documentada de controles por oposición de intereses realizados por sectores independientes. Los mismos deben mantenerse por un plazo no inferior a 2 (dos) años, para su posterior revisión por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

2.5.4. Actividades y segregación de funciones. Incompatibilidades.

	Análisis funcional / Programación	Control de calidad	Operaciones	Administración de resguardos	Implementaciones	Data Entry	Administración de bases de datos	Administración de redes	Administración de telecomunicaciones	Administración del sistema operativo	Mesa de ayuda	Usuario final	Asignación de perfiles	Definición e implementación de políticas, perfiles y accesos	Control y monitoreo de seguridad informática
Análisis funcional / Programación		X	NO	NO	NO		NO	X	X	NO		NO	NO	NO	NO
Control de calidad	X		NO	NO	X	X	NO	X	X	NO	NO		NO	NO	NO
Operaciones	NO	NO			X	NO	X	X	X	X		NO	NO	NO	NO
Administración de resguardos	NO	NO			X	NO	NO			X	NO	X	NO	NO	NO
Implementaciones	NO	X	X	X		NO	NO			X	X	NO	NO	NO	NO
Data Entry		X	NO	NO	NO		NO	X	X	X	X		NO	NO	NO
Administración de bases de datos	NO	NO	X	NO	NO	NO				X	X	NO	NO	NO	NO
Administración de redes	X	X	X			X						NO	NO	NO	NO
Administrador de comunicaciones	X	X	X			X						NO	NO	NO	NO
Administración de sistemas operativos	NO	NO	X	X	X	X	X					NO	NO	NO	NO
Mesa de ayuda		NO		NO	X	X	X					NO	NO	NO	NO
Usuario final	NO		NO	X	NO		NO	NO	NO	NO	NO			NO	NO
Asignación de perfiles	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO				
Definición e implementación de políticas, perfiles y accesos	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			
Control y monitoreo de seguridad informática	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			

2.5.5. Glosario de funciones descriptas en el cuadro del punto 2.5.4.:

Análisis de sistemas / programación: diseño y desarrollo de los sistemas aplicativos, de acuerdo con las necesidades del negocio y del usuario.

Control de calidad: prueba y homologación de software de aplicación para la puesta en producción.

Operaciones: gestión operativa del procesamiento de información y el equipamiento afectado.

Administración de resguardos: custodia, guarda y mantenimiento de los archivos de datos y programas almacenados en distintos medios.

Implementaciones: puesta en producción de sistemas aplicativos.

Data entry: recepción y carga a los sistemas de lotes de información para su posterior procesamiento.

Administración de bases de datos: definición y mantenimiento de la estructura de los datos de las aplicaciones que utilizan este tipo de software.

Administración de redes: administración y control técnico de la red local.

Administración de telecomunicaciones: administración y control técnico de la red WAN.

Administración de sistemas operativos (system programming): mantenimiento del software de sistemas operativos.

Mesa de ayuda: canalización de respuestas a inquietudes técnicas de los usuarios.

Usuario final: aquel que hace uso de los sistemas aplicativos.

Asignación de perfiles: vinculación de los usuarios finales con los perfiles de las funciones que aquellos pueden realizar.

Definición e implementación de políticas, perfiles y accesos: diseño y puesta operativa de las políticas y los procedimientos de seguridad, de la creación y mantenimiento de los perfiles de usuario y de la asignación de los permisos a los activos de información.

Control y monitoreo de seguridad informática: seguimiento de las actividades relacionadas con el empleo de los activos de información.

3.1. Gestión de la seguridad.

3.1.1. Dependencia del área responsable.

Las entidades financieras deben considerar en su estructura organizacional un área para la protección de los activos de información, con el fin de establecer los mecanismos para la administración y el control de la seguridad sobre el acceso lógico y físico a sus distintos ambientes tecnológicos y recursos de información: equipamiento principal, plataforma de sucursales, equipos departamentales, subsistemas o módulos administradores de seguridad de los sistemas de aplicación, sistemas de transferencias electrónicas de fondos, bases de datos, canales de servicios electrónicos, banca por Internet y otros.

El responsable de la protección de activos de información gestionará la implementación y el mantenimiento de la política de seguridad para los mismos, establecida por el Directorio, o autoridad equivalente de la entidad.

La ubicación jerárquica del área deberá garantizar, en forma directa, su independencia funcional y operativa de las áreas de tecnología y sistemas de información, del resto de las áreas usuarias y de la función de auditoría.

Deben definirse, documentarse y asignarse adecuados roles para los recursos humanos que la integran, considerando: misiones y funciones, responsabilidades, habilidades necesarias para cubrir el puesto y otros aspectos que las entidades financieras crean relevantes. Los recursos humanos que desempeñen la función deben contar con adecuados niveles de entrenamiento en la implementación de controles y el mantenimiento de políticas y sanas prácticas de seguridad.

3.1.2. Estrategia de seguridad de acceso a los activos de información.

De acuerdo con sus operaciones, procesos y estructura, las entidades financieras deben definir una estrategia de protección de activos de información, que les permita optimizar la efectividad en la administración y el control de sus activos de información.

Dicha estrategia debe considerar las amenazas y las vulnerabilidades asociadas a cada entorno tecnológico, su impacto en el negocio, los requerimientos y los estándares vigentes. Para ello deben asignar claramente roles y responsabilidades en materia de seguridad, comprometiendo a los máximos niveles directivos y gerenciales.

La estrategia de seguridad deberá contemplar el establecimiento de mecanismos de control para la detección, registro, análisis, comunicación, corrección, clasificación y cuantificación de los incidentes y de las debilidades en los accesos no autorizados a la información administrada en los sistemas de información.

Se valorará que la mencionada estrategia abarque, además de los recursos informáticos propios de la entidad, a sus grupos de influencia: sistema financiero, clientes de todo tipo, proveedores de recursos y sistemas de información, operadores de telecomunicaciones, requerimientos de los organismos de regulación y control, y otros entes externos vinculados directa o indirectamente.

3.1.3. Planeamiento de los recursos.

En los ciclos de gestión de las funciones informáticas, se deben considerar el planeamiento, la implementación y el mejoramiento continuo de los procesos de administración y control de seguridad sobre la protección de activos de información.

De acuerdo con los riesgos identificados en las metas y planes estratégicos, se deben elaborar planes operativos que contemplen los factores críticos para un efectivo control de las aplicaciones junto con las actividades del negocio que respaldan. Dichos planes operativos tendrán en cuenta las tareas a realizar con su correspondiente asignación de tiempos y recursos, las prioridades y la precedencia de cada una de ellas.

En los nuevos proyectos informáticos se deben contemplar los requerimientos de seguridad desde sus etapas iniciales, con el objetivo de asegurar el diseño y la implementación de apropiados controles y registros de seguridad, como así la correcta selección de tecnología que haga a la solución integral de la misma.

3.1.4. Política de protección.

De acuerdo con su estrategia de seguridad, las entidades financieras deben desarrollar una política de protección de los activos de información. Ésta debe evidenciar claramente que es un instrumento que se utiliza para proporcionar dirección y apoyo gerencial con el objeto de brindar protección de los activos de información. Además, identificará los recursos críticos a proteger y los riesgos internos y externos de accesos no autorizados sobre los mismos.

El Directorio, o autoridad equivalente, deberá establecer una dirección política clara, y demostrar apoyo y compromiso con respecto a la protección de los activos de información, mediante la formulación, aprobación formal y difusión de la misma a través de toda la entidad.

Deberá ser implementada y comunicada a todo el personal y servir como base para el desarrollo de las normas, los manuales, los estándares, los procedimientos y las prácticas que gobiernen los aspectos de seguridad de los sistemas de información, los datos y la tecnología informática asociada.

La mencionada documentación deberá contemplar, como mínimo:

- objetivo, alcance, principios y requisitos de seguridad de acceso lógico;
- acuerdos, términos y condiciones de confidencialidad de los datos;
- procedimientos para la implementación de nuevos recursos y servicios de información;
- estándares para la clasificación de los activos de información (recursos tecnológicos, datos y ambientes físicos);
- procedimientos para el acceso y la autenticación de los usuarios;
- procedimientos para la generación y distribución de usuarios y claves de identificación personal (contraseñas, PIN, *tokens*, otros similares) para el ingreso a los sistemas;

- sanas prácticas de seguridad para la utilización y selección de claves de identificación personal;
- procedimientos para la comunicación de incidentes y debilidades relacionados con accesos no autorizados, pérdidas o daños a la información;
- mecanismos para la asignación y la utilización de los usuarios especiales y de contingencia;
- estándares para el empleo de aquellos utilitarios que permitan el alta, la baja o la modificación de datos operativos, por fuera de los sistemas aplicativos que los originan;
- procedimientos de control de cambios y puesta en producción de programas;
- procedimientos para el registro y comunicación de incidentes en materia de seguridad;
- prácticas de seguridad para la utilización del correo electrónico y navegación por Internet;
- procedimientos para la prevención, detección y eliminación de software malicioso,
- procedimiento a seguir para la detección de intrusos en las redes y plataformas informáticas, así como las acciones que deben implementarse luego de su detección;
- pautas mínimas de seguridad a contemplar en la adquisición de nuevos recursos tecnológicos, sistemas aplicativos y software de base, y
- toda aquella documentación que se considere relevante de acuerdo con las características propias de administración y control informático.

La política de seguridad y los documentos que la complementan deben someterse periódicamente a procesos de revisión y actualización, de acuerdo con la evaluación de riesgos y la complejidad de la entidad financiera, asegurando la correcta implementación de mejores prácticas de seguridad informática en los circuitos operativos y ambientes computadorizados de información. Asimismo, la mencionada documentación se deberá reconsiderar ante la implementación de nuevos programas y sistemas, cambios en las operaciones, actualizaciones tecnológicas y nuevas relaciones con terceros.

3.1.4.1. Clasificación de los activos de información - Niveles de acceso a los datos.

Las entidades financieras deben clasificar sus activos de información de acuerdo con su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados en sus sistemas de información.

Esta clasificación deberá ser documentada, formalizada y comunicada a todas las áreas de la entidad, principalmente a los propietarios de los datos. La misma puede ser parte integrante de la política de protección de los activos de información, o formar un documento aparte.

Los niveles de acceso deben diseñarse considerando los criterios de la clasificación, junto con una adecuada separación de tareas, determinando qué clases de usuarios o grupos poseen derechos de acceso -y con qué privilegio- sobre los datos, sistemas, funciones y servicios informáticos.

La asignación de derechos de acceso debe otorgarse a través de un proceso de autorización formal del propietario de los datos, verificando periódicamente los niveles y privilegios otorgados a los usuarios.

3.1.4.2. Estándares de acceso, de identificación y autenticación, y reglas de seguridad.

Se deben implementar métodos de identificación y autenticación para controlar el acceso lógico a los sistemas y servicios informáticos, los que dependerán de la criticidad y el valor de los datos a proteger, debiéndose considerar:

- la modificación de las contraseñas maestras y de cuentas especiales "por defecto" de los sistemas operativos, de los subsistemas administradores de seguridad, de las bases de datos y de las herramientas para la administración y el control;
- el cambio obligatorio de las contraseñas de acceso en el primer inicio de sesión;
- 8 (ocho) caracteres de longitud para las claves provistas a todo sistema informático de la entidad;
- el control de la composición de las contraseñas (por ejemplo: caracteres alfabéticos, numéricos, especiales, mayúsculas y minúsculas);
- el registro histórico de las últimas 12 (doce) contraseñas utilizadas, evitando ser reutilizadas;
- el intervalo de caducidad automática de las mismas a los 30 (treinta) días;
- el bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso fallidos;
- la desconexión automática de la sesión de usuario en la aplicación y en la red por tiempo de inactividad a los 15 (quince) minutos;
- la eliminación de las cuentas de usuario inactivas por un período mayor a 90 (noventa) días;
- la no utilización de denominaciones de usuario genérico para perfiles asignados a personas físicas;
- técnicas de encriptación, con algoritmos de robustez reconocida internacionalmente, para el archivo de las contraseñas;
- asignación de contraseñas para todas las cuentas;
- restricción de accesos concurrentes;
- la identificación única (ID) de usuarios;
- definición de opciones y menús para acceder a las funciones de los sistemas de información;
- la dinámica en la actualización de los derechos de acceso, revocando los usuarios que se desvincularan de la entidad y modificando los perfiles de aquellos que cambiaron de función;
- la permanente actualización de los sistemas operativos y herramientas con respecto a nuevas vulnerabilidades, y "*patches*".

Asimismo, se consideran sanas prácticas de seguridad:

- el mantenimiento de la información codificada por mecanismos de encriptación en los sistemas de bases de datos;
- la utilización de adecuadas herramientas para la administración y el control de la seguridad de acceso;
- la permanente actualización de las versiones de los sistemas operativos;

- la deshabilitación de los accesos remotos a los recursos de información;
- la utilización de restricciones en los días y horarios de conexión;
- la verificación de la identidad del usuario ante solicitudes de reactivación de cuentas;
- el uso de estándares nemotécnicos para los perfiles de acceso de usuarios, grupos y recursos de sistemas;
- el empleo de mecanismos de autenticación biométrica;
- la utilización de smart-cards como dispositivos de identificación de accesos;
- la utilización de “single sign-on”, y
- la permanente incorporación de prácticas y estándares reconocidos de seguridad.

3.1.4.3. Programas de utilidad con capacidades de manejo de datos - Usuarios privilegiados y de contingencia.

Deben implementarse adecuadas restricciones para el empleo de los programas que permitan el alta, la baja o la modificación de datos operativos por fuera de los sistemas aplicativos, en las distintas plataformas.

Asimismo, deben desarrollarse mecanismos formales para la asignación y la utilización de usuarios especiales con capacidades de administración, que puedan ser usados en caso de emergencia o interrupción de las actividades. Los usuarios definidos con estas características deben contar con adecuadas medidas de resguardo y acceso restringido. Su utilización será registrada y se realizarán controles posteriores sobre los reportes de eventos, analizando la concordancia entre las tareas realizadas y el motivo por el cual se los solicitó.

3.1.4.4. Registros de seguridad y pistas de auditoría.

Con el objeto de reducir a un nivel aceptable los riesgos internos y externos de accesos no autorizados, pérdidas y daños a la información, se deben implementar adecuadamente:

- registros operativos de las actividades de los usuarios, las tareas realizadas y las funciones utilizadas;

- reportes de seguridad que registren la asignación de claves y derechos de accesos, empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones, actividades de los usuarios privilegiados, usuarios de emergencia y con accesos especiales, intentos fallidos de acceso y bloqueos de cuentas de usuario, y

- reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.

Se deberá proteger la integridad de la información registrada en dichos reportes, la que deberá ser resguardada adecuadamente, manteniéndose en archivo por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dichos registros de seguridad o pistas de auditoria, podrá ser inferior a 6 (seis) años. Para ello, se utilizarán soportes de almacenamiento no modificables o soportes reutilizables, siempre que se proteja la integridad de la información con medidas de control que permitan evidenciar la no alteración posterior a su generación. En caso de ser CD (Compact Disc), deberá registrarse oportunamente el número de serie del mismo al momento de generación y/o firmas digitales.

3.1.4.5. Alertas de seguridad y software de análisis.

Las entidades financieras deben implementar funciones de alertas de seguridad y sistemas de detección y reporte de accesos sospechosos a los activos de información, y contar con monitoreo constante de los accesos a recursos y eventos críticos, que reporten a los administradores sobre un probable incidente o anomalía en los sistemas de información.

Asimismo, se considera una sana práctica de seguridad la detección en tiempo real de los eventos o intrusiones, así como la utilización de herramientas automatizadas para el análisis de la información contenida en los registros operativos, de seguridad y de auditoría. De esta manera, se reducirá el volumen de los datos contenidos en los reportes, minimizando los costos relacionados con su almacenamiento y tareas de revisión.

3.1.4.6. Software malicioso.

Las entidades financieras deben implementar adecuados mecanismos de protección contra programas maliciosos, tales como: virus informáticos, “gusanos” de red, “spyware”, “troyanos”, y otros que en el futuro puedan surgir, con el objeto de prevenir daños sobre los datos y la pérdida de información. Deben desarrollar procedimientos de difusión a los usuarios de los sistemas de información y a los recursos humanos de las áreas técnicas, sobre sanas prácticas en materia de prevención.

Deben implementarse herramientas para la prevención, detección y eliminación de este tipo de software en los distintos ambientes de procesamiento, evitando su propagación y replicación a través de las redes informáticas, archivos y soportes de información. Estas herramientas deben actualizarse rutinariamente contra nuevas amenazas.

Deberán definirse controles de seguridad para prevenir la presencia de código malicioso en archivos adjuntos a correos electrónicos y en los accesos a Internet; asimismo, se deberá impedir la instalación y utilización de software no autorizado.

3.1.5. Responsabilidades del área.

El área será responsable de observar la existencia y correcta aplicación de los controles considerados como práctica recomendada y de uso frecuente en la implementación de la protección de los activos de información. Los mismos comprenden:

- la existencia de una política de protección de los activos de información, correctamente redactada, formalizada, actualizada y comunicada a toda la entidad;
- la asignación de responsabilidades operativas en materia de administración de la protección de los activos de información;
- la comunicación oportuna de incidentes relativos a la seguridad, a los responsables propietarios de los datos;
- la existencia de procedimientos de control y monitoreo, y su aplicación, sobre el empleo continuo de los estándares fijados de seguridad;
- la instrucción y el entrenamiento en materia de seguridad de la información.

Adicionalmente, los controles efectuados por el área deben establecerse formalmente a través de reportes operativos, que permitan la supervisión continua y directa de las tareas y el análisis del logro de las metas definidas. Estos reportes deben mantenerse en archivo por un término no menor a 2 (dos) años, utilizando para ello soportes de almacenamiento no reutilizables y preferentemente sometidos a algoritmos de función irreversible o como normalmente se denomina “funciones hash”.

De acuerdo con el marco definido en la política de seguridad informática, las entidades financieras deben desarrollar e implementar controles precisos, oportunos y eficaces sobre las funciones de acceso a los datos y a los recursos de información.

3.1.5.1. Control y monitoreo.

El área de protección de activos de información es la responsable primaria de efectuar las actividades regulares de monitoreo y controles de verificación. La frecuencia de revisión dependerá del valor de la información administrada y del riesgo asociado a la aplicación o servicio tecnológico.

Se deben evaluar los accesos a las funciones de administración y procesamiento de los programas de aplicación y sus registros de datos resultantes. Asimismo, se deben controlar especialmente los usuarios con niveles de accesos privilegiados, su utilización y su asignación.

Los incidentes y debilidades en materia de seguridad deben registrarse y comunicarse inmediatamente a través de adecuados canales de información, con el objeto de analizar sus causas e implementar mejoras en los controles informáticos a fin de evitar su futura ocurrencia.

3.2. Implementación de los controles de seguridad física aplicados a los activos de información.

Los recursos humanos, los equipos, los programas, los archivos y los datos que involucran a las operaciones y procesos de la tecnología de la información representan uno de los activos críticos de las entidades financieras. El Directorio, o autoridad equivalente, es el responsable primario por la existencia de distintos niveles de seguridad física en correspondencia con el valor, confidencialidad y criticidad de los recursos a proteger y los riesgos identificados.

Los datos y equipos considerados críticos deben ser instalados en ambientes conforme a estándares y normas nacionales e internacionales pertinentes, que protejan a los mismos contra fuego, calor, humedad, gases corrosivos, acceso indebido, desmagnetización y todo otro tipo de evento que pueda afectarlos.

El Directorio, o autoridad equivalente, debe considerar el uso de sistemas de monitoreo centralizado en todas las facilidades, con el objetivo de lograr un control preventivo y correctivo de fallas en la seguridad. Además, se valorará la inclusión de dispositivos de video y grabación de eventos en aquellas áreas con mayor concentración de activos de información.

3.2.1. Construcción y localización de las instalaciones.

Será ponderado como una buena práctica en la administración del riesgo que la localización del centro de procesamiento de datos esté en un área que resulte de difícil identificación pública.

No deben admitirse ambientes compartidos que permitan la exposición de las operaciones críticas y de carácter confidencial de la entidad financiera, a personas, materiales u otro tipo agentes externos. Esas operaciones deben realizarse en ambientes seguros, con un nivel de protección probadamente eficaz contra las amenazas de su entorno, con el propósito de preservar la integridad de los datos y dispositivos de hardware.

Las instalaciones del centro de procesamiento de datos, además de los niveles de protección físico-ambiental adecuados, deben tener en cuenta, entre otras, las siguientes consideraciones, relevantes para los controles de seguridad física:

- instalaciones para equipamientos de apoyo, tales como: equipos de aire acondicionado, grupos generadores, llaves de transferencia automática, UPS, baterías, tableros de distribución de energía y de telecomunicaciones y estabilizadores;
- instalaciones de montaje apropiadas para los sistemas de telecomunicaciones;
- instalaciones de montaje apropiadas para los sistemas de suministro eléctrico, tanto primario como secundario;
- iluminación de emergencia;
- sistemas de monitoreo y control de las utilidades críticas del centro de procesamiento de datos; y,

- se valorizará toda otra medida adoptada para minimizar los riesgos que afecten a los recursos de tecnología.

3.2.2. Acceso físico a las instalaciones del centro de procesamiento de datos.

Las instalaciones deben tener apropiados controles de acceso, por medio de los cuales se permita sólo el ingreso al área de procesamiento de datos a personal autorizado.

Se valorizará la existencia de varios niveles de acceso para los distintos recintos del centro de procesamiento de datos, basados en las definiciones de necesidad de acceder, en relación con la función o actividad primaria del personal interno o externo a la entidad financiera que solicite el ingreso.

Todos los accesos, de rutina o de excepción, deben ser registrados por mecanismos que permitan la posterior revisión de los siguientes datos como mínimo: nombre completo, relación (interno o externo), en caso de ser externo deberá constar quién ha autorizado el acceso, motivo, hora de ingreso y hora de egreso.

3.2.3. Mecanismos de protección ambiental.

Los sistemas de prevención contra incendios en los ambientes de procesamiento de datos deben posibilitar alarmas preventivas, que tengan la capacidad de ser disparadas ante la presencia de partículas características en el recalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

Los materiales combustibles deben ser minimizados dentro del área del centro de procesamiento de datos. La mampostería, muebles y útiles deben ser constructivamente no inflamables, y preferentemente ignífugos.

Se considerarán como ventajosas la aplicación de sanas prácticas de control para minimizar el riesgo de amenazas potenciales, la implementación de detectores ante: robo, presencia de agua (o falta de suministro), polvo, vibraciones, sustancias químicas, interferencia en el suministro de energía eléctrica, radiación electromagnética; y otras medidas similares.

3.2.4. Destrucción de residuos y de medios de almacenamiento de información

Todos los documentos en papel que contengan informaciones clasificadas como críticas deben ser triturados o destruidos, a efectos de imposibilitar su lectura, antes de ser desechados.

Todos los dispositivos electrónicos que ya no se utilicen, y que hayan sido funcionales para el almacenamiento de información crítica deben ser físicamente destruidos antes de su desecho.

4.1. Responsabilidades sobre la planificación de la continuidad del procesamiento de datos.

El Directorio, o autoridad equivalente de la entidad financiera, es el responsable primario por la identificación, la valorización, la gestión y el control de los riesgos. Debe asegurar la existencia y la provisión de los recursos necesarios para la creación, mantenimiento y prueba de un plan de recuperación del procesamiento electrónico de datos. El mismo deberá ser operable y funcional, acorde a los requerimientos de negocio de la entidad financiera y de los organismos de control.

Deberá designarse formalmente un área o sector, que será responsable de la creación, mantenimiento y prueba satisfactoria del plan de recuperación del procesamiento electrónico de datos.

La continuidad es considerada como un proceso que se inicia con la recuperación durante la contingencia, y concluye con la vuelta a la normalidad una vez controladas las causas que generaron dicha contingencia.

4.2. Análisis de impacto.

La continuidad del procesamiento electrónico de datos, que en definitiva posibilita la continuidad de los negocios, deberá evidenciar que se han identificado los eventos que puedan ocasionar interrupciones en sus procesos críticos.

Es responsabilidad del Directorio, o autoridad equivalente, observar que se haya llevado a cabo una evaluación de riesgos para determinar el impacto de distintos eventos, tanto en términos de magnitud de daño como del período de recuperación y la vuelta a la normalidad.

Estas dos actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. La evaluación considerará todos los procesos de negocio y no se limitará sólo a las instalaciones de procesamiento de la información, sino también a todos los recursos relacionados.

Los resultados de la evaluación deben ser el soporte para la selección de mecanismos alternativos de recuperación y adopción de medidas preventivas para la confección del plan de recuperación y vuelta a la normalidad del procesamiento de datos.

Dichos resultados serán formalmente aprobados y tomados en conocimiento por el Directorio, o autoridad equivalente de la entidad financiera, y deben estar disponibles en forma permanente para ser auditados por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

4.3. Instalaciones alternativas de procesamiento de datos.

Las instalaciones alternativas de procesamiento de datos deben atender los requisitos mínimos establecidos por estas normas, pudiendo ser propias o de terceros.

El equipamiento de las instalaciones de procesamiento alternativo debe contemplar la capacidad de administración y gestión de todos los procesos de negocios clasificados como críticos para asegurar la actividad de la entidad financiera.

En el caso en que la entidad financiera cuente con sucursales, la instalación alternativa debe prever la existencia de equipamiento destinado a las telecomunicaciones para acceder al servicio mínimo de las mismas.

En caso de un siniestro o suceso contingente que torne inoperantes las instalaciones principales, la localización de las instalaciones alternativas deberá ser tal que no sean alcanzadas por el mismo evento. Además, deberán tornarse totalmente operacionales en condiciones idénticas, en una ventana de tiempo tal que no afecte la atención de los clientes, ni deje a la entidad fuera del proceso de compensación.

La selección de la localización antes mencionada deberá estar soportada por la evidencia documental de la existencia de un análisis de riesgo de eventos simultáneos, que estarán fehacientemente expresados en el mismo.

4.4. Plan de continuidad del procesamiento de datos.

Se debe evidenciar la existencia de un procedimiento escrito, aprobado formalmente, para atender a la continuidad del procesamiento de datos y actividades vinculadas, en el caso que se presenten contingencias o emergencias.

El documento deberá basarse en el mismo análisis de riesgo efectuado para determinar la localización de las instalaciones alternativas de procesamiento de datos, enunciando todos los posibles escenarios que harían que el plan entrara en funcionamiento.

El mismo deberá, como mínimo, contener lo siguiente:

- Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente. Estos deben incluir disposiciones con respecto a la gestión de vínculos eficaces a establecer con las autoridades públicas pertinentes, por ej.: entes reguladores, policía, bomberos y otras autoridades.

- Los nombres, direcciones, números de teléfono y "localizadores" actuales del personal clave.

- Las aplicaciones criticas y su prioridad con respecto a los tiempos de recuperación y regreso a la operación normal.

- El detalle de los proveedores de servicios involucrados en las acciones de contingencia / emergencia.

- La información logística de la localización de recursos claves, incluyendo: ubicación de las instalaciones alternativas, de los resguardos de datos, de los sistemas operativos, de las aplicaciones, los archivos de datos, los manuales de operación y documentación de programas / sistemas / usuarios.

- Los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales a las ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos.
- La inclusión de los planes de reconstrucción para la recuperación en la ubicación original de todos los sistemas y recursos.
- Todo otro recurso definido como soporte de los procesos de negocio a recuperar.

4.5. Mantenimiento y actualización del plan de continuidad de procesamiento de datos.

El plan de continuidad del procesamiento electrónico de datos debe mantenerse por medio de revisiones y actualizaciones periódicas para garantizar su eficacia permanente. Se debe evidenciar que existen procedimientos escritos a fin de asegurar que todo cambio en los procesos de negocio y en su tecnología relacionada se reflejen en las actualizaciones sobre el plan de continuidad.

Debe existir un responsable formalmente identificado para el mantenimiento y adecuación del plan de continuidad, al cual deberá asignarse la responsabilidad de las revisiones periódicas, la identificación de cambios y su actualización. Este proceso formal de control de cambios debe garantizar que se distribuya el plan actualizado a todos los responsables involucrados en el mismo.

4.6. Pruebas de continuidad del procesamiento de datos.

El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben permitir asegurar la operatoria integral de todos los sistemas automatizados críticos –de acuerdo con los análisis de riesgo previos-, a efectos de verificar que el plan está actualizado y es eficaz. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente del plan mencionado.

Deberá evidenciarse la existencia de un cronograma formal de pruebas que indicará cómo debe probarse cada elemento del plan, y la fecha en la cual cada una de las pruebas deberá ser efectuada.

En las pruebas deben participar las áreas usuarias de los procesos de negocio, quienes deben verificar los resultados de las mismas. Se deberá documentar formalmente su satisfacción con el resultado de la prueba como medio para asegurar la continuidad de los procesos de negocio en caso de que ocurra una contingencia. La auditoría interna de la entidad también deberá conformar la satisfacción por el resultado de las mismas a tal efecto.

El informe realizado por las áreas usuarias y de auditoría interna deberá ser tomado en conocimiento por el Directorio, o autoridad equivalente de la entidad, y mantenido en archivo para su control posterior por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.1. Responsabilidad del área.

El área de operaciones deberá evidenciar la existencia de un responsable único para la gestión, el control y el reporte de los centros productivos de procesamiento de datos, sean estos centralizados o distribuidos. La gestión operativa deberá asegurar el normal funcionamiento de la infraestructura de sistemas de información y la tecnología relacionada.

5.2. Inventario tecnológico.

Las entidades financieras deben contar con la capacidad de identificar sus activos informáticos y de información, las características, la localización y la criticidad e importancia de los mismos.

Sobre la base de esta información, las entidades financieras podrán asignar niveles de protección proporcionales a la importancia de los activos, realizar una continua categorización de los mismos, mantenerlos actualizados y efectuar el mantenimiento preventivo de sus recursos físicos.

Por ello, las entidades financieras deben elaborar y mantener un inventario de los activos asociados a cada sistema de información. Se debe identificar claramente cada activo, estableciendo su propietario y su clasificación en cuanto a seguridad.

El inventario, como mínimo, debe contener los siguientes elementos:

- recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia;
- activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems, otros), equipos de comunicaciones (routers, firewalls, switches, encriptadores, otros), medios magnéticos (cintas, discos, resguardos varios), otros equipos técnicos;
- servicios descentralizados en terceros: servicios informáticos y de comunicaciones, fabricas de software, otros.

5.3. Políticas y procedimientos para la operación de los sistemas informáticos y manejadores de datos.

Debe existir una adecuada planificación, y documentación escrita y actualizada, de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberán incluir -como mínimo- el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos para el registro de los eventos y problemas, los procedimientos sobre cancelaciones y reproceso en cada una de las actividades, las relaciones con otras áreas y los mecanismos de distribución de la información.

Deben establecerse procedimientos de control para garantizar la efectiva y correcta realización de cambios cuando corresponda, por ejemplo: modificaciones de programas en bibliotecas de producción o archivos, definiciones de diccionarios de datos, órdenes de corrida de programas, etc.

5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.

El Directorio, o autoridad equivalente, es el responsable primario de la existencia de soluciones para el almacenamiento y resguardo de datos, programas y todo otro componente de información relevante para las funciones de negocio, para las acciones de recuperación del procesamiento de datos en caso de contingencias, de necesidades de reproceso y por requisitos de disposiciones legales y reguladoras.

Deberá evidenciarse la existencia de procedimientos donde esté formalmente documentada la metodología de resguardos utilizada, las responsabilidades del personal apropiado, las prioridades de resguardo, los ciclos de rotación, los lugares de almacenamiento, las convenciones de rotulación. Además, deberán establecer la frecuencia de las pruebas sobre los resguardos, el mecanismo de selección de resguardos históricos para la realización de las mismas, la participación de los usuarios propietarios de los datos en ellas, y otros puntos que la entidad considere relevantes.

Las pruebas de recuperación y de integridad de los resguardos de datos deben ser formalizadas y debidamente documentadas. Las pruebas deben abarcar tanto resguardos actuales como históricos. Las mismas deben contemplar la antigüedad y el medio de almacenamiento utilizado. La documentación del resultado de las pruebas debe evidenciar la participación y conformidad por los resultados obtenidos de los usuarios propietarios de los datos.

Los períodos de retención de los resguardos de datos, programas y todo otro componente de información (diarios, semanales, mensuales, etc.) deben asegurar la recuperación de los mismos ante cualquier inconveniente de procesamiento que se presente al momento más cercano anterior el evento contingente.

Los procedimientos para el resguardo de datos, programas y todo otro componente de información deben prever, como mínimo, la generación de 2 (dos) copias de resguardos sincronizadas, manteniendo el almacenamiento de una de ellas en una localización distinta a la primaria, ubicada a una distancia determinada de acuerdo con el análisis de riesgos simultáneos que la entidad haya formalmente realizado.

Cuando sea factible, las entidades financieras podrán desarrollar mecanismos de redundancia automática para los resguardos de datos (duplicado o espejado on-line), cuyo alcance deberá abarcar tanto resguardos actuales como históricos. En dicho caso, este resguardo podrá ser considerado como una de las copias enunciadas en el párrafo anterior.

Se deberán mantener inventarios de todos los resguardos, tanto en el sitio primario como en el secundario, con clara identificación de su denominación nemotécnica, el tipo de contenido, la fecha de resguardo, los ciclos de rotación, períodos de retención, cantidad de usos del medio, fecha esperada de destrucción, responsable del resguardo, fecha de última prueba del resguardo, responsable de la prueba, y otros datos que la entidad financiera considere relevantes.

5.5. Mantenimiento preventivo de los recursos tecnológicos.

Se deberá observar la existencia de una política para la realización de mantenimiento preventivo de los recursos tecnológicos que soportan a los sistemas de información y de los recursos relacionados. También se crearán procedimientos formales para llevar a cabo dicha tarea, que contarán con cronogramas de mantenimiento. Se deben documentar las tareas realizadas y mantener en archivo los reportes, como mínimo por el doble del período que se haya fijado para el ciclo de mantenimiento.

Los cronogramas de mantenimiento deben estar coordinados con los de producción a fin de no impactar en la operatoria normal.

Cuando las tareas de mantenimiento sean efectuadas por recursos humanos externos, deben contemplarse las medidas de control de acceso físico enunciadas en la presente.

5.6. Administración de las bases de datos.

Las bases de datos son, en casi todos los casos, el repositorio de la información crítica de las entidades financieras. Las fallas en el manejo de las mismas pueden ocasionar, en forma intencional o no, la modificación no autorizada, la destrucción o exposición de datos e información crítica.

Los responsables del área de protección de activos de información y el área de operaciones y procesamiento de datos deben considerar cuidadosamente las implicancias en la seguridad de los sistemas administradores de bases de datos.

Muchas veces, los sistemas de administración de bases de datos (DBMS) cuentan con la posibilidad de mantener un registro de los accesos que se han realizado a las bases, en todos sus niveles, pero son desactivados.

Sin embargo, estos sistemas brindan la posibilidad de modificar, agregar o eliminar datos. Adicionalmente, es posible modificar derechos de acceso a los mismos, con el consecuente riesgo que esto implica cuando se ha imposibilitado el control de las actividades efectuadas sobre las bases de datos.

En todos los casos se deberá evidenciar la existencia de un fuerte control por oposición de responsabilidades en las actividades que realizan los encargados de gestionar los sistemas administradores de las bases mencionadas. Los controles ejercidos deben estar en concordancia con la frecuencia de administración de los DBMS, ser formalmente documentados, y en caso de no ser efectuados por el área de protección de activos de información, deben ser reportados a ella, en especial cuando se detecten distorsiones en el uso normal o intrusiones sobre los datos.

Los reportes deben ser mantenidos al menos por 2 (dos) años, a efectos de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.7. Gestión de cambios al software de base.

Se deben controlar los cambios en el software de base e instalaciones de procesamiento de información.

Se deben establecer responsabilidades y procedimientos formalmente documentados, para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software de base o los procedimientos operativos de procesamiento por lotes. Los sistemas operativos deben estar sujetos a un control estricto de los cambios. Cuando se cambien los programas, se debe retener un registro de auditoría que contenga toda la información relevante.

Los procedimientos deben contemplar e identificar las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Los cambios en el ambiente operativo pueden tener impacto en las aplicaciones. Por este motivo, se debe considerar la existencia -como mínimo- de la siguiente información:

- aprobación formal de los cambios propuestos;
- identificación y registro de los cambios significativos realizados;
- comunicación de detalles de cambios a todas las áreas pertinentes.

Esta documentación deberá ser mantenida, como mínimo por 2 (dos) años, a efecto de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.8. Control de cambios a los sistemas productivos.

A fin de minimizar el riesgo de actualizaciones accidentales en el entorno productivo, ingresar programas no probados y evitar accesos no autorizados a los datos, las entidades financieras deben definir un adecuado esquema de separación entre sus ambientes informáticos de procesamiento (desarrollo, prueba y producción). Se deberá asegurar que los analistas y programadores de sistemas no tengan acceso al entorno productivo, ni los operadores accedan al ambiente ni a las herramientas utilizadas para el desarrollo y el mantenimiento de los sistemas de aplicación, de acuerdo con el cuadro del punto 2.5.4. sobre segregación de funciones.

El proceso de actualización de nuevas versiones de sistemas deberá ser estrictamente controlado y realizado por personal que no tenga relación con el área de desarrollo y mantenimiento, mediante mecanismos que garanticen la correspondencia entre los programas "fuentes" y los programas "ejecutables".

Asimismo, las nuevas versiones y las modificaciones de los programas aplicativos deben someterse a procedimientos formales de revisión, registro y aprobación, antes de la implementación definitiva en el ambiente de producción.

En los casos de implementaciones de sistemas informáticos adquiridos, desarrollados o mantenidos por servicios externos, se deben registrar adecuadamente los cambios efectuados, verificando que todos los programas "fuentes" en custodia se correspondan con los programas "ejecutables", antes de su puesta operativa en el ambiente de producción.

5.9. Mecanismos de distribución de información.

La información generada por los sistemas informáticos, sea ésta en medios electrónicos o en copias impresas, deberá contemplar los recaudos mínimos de seguridad a efectos de impedir su difusión a personas no autorizadas.

Los responsables del área de protección de activos de información y el área de operaciones y procesamiento de datos son responsables del análisis y la implementación de los controles necesarios para limitar la pérdida de confidencialidad en la distribución de la información, tanto dentro como fuera de la entidad financiera.

Se valorará la aplicación de medidas tales como: utilización de sobres cerrados, cofres de seguridad para el transporte, el acceso limitado a los nichos de distribución de listados y la seguridad en las comunicaciones de los medios que soportan información.

5.10. Manejo de incidentes.

Se debe evidenciar la existencia de procedimientos formalmente documentados para la gestión, registro, accionar y comunicación de anomalías de los sistemas productivos y de software de base.

Se deben considerar, como mínimo, las siguientes acciones:

- advertir y registrar los síntomas del problema y los mensajes que aparecen en pantalla, fecha y hora del incidente;
- dejar constancia de la comunicación a los sectores responsables de la resolución;
- documentar las acciones realizadas, fecha y hora de la resolución.

Asimismo, deben implementarse adecuados procesos de respuesta para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados los mismos.

5.11. Medición y planeamiento de la capacidad.

El área de operaciones y procesamiento de datos deberá evidenciar la realización de análisis y planificación de capacidad, los que deben contemplar los planes estratégicos de la entidad financiera, la expansión de la base de clientes activos, los nuevos productos y servicios, la implementación de nueva tecnología y la adición de nuevos usuarios, entre otros factores.

5.12. Soporte a usuarios.

Deberá existir una función -que, de acuerdo con la complejidad que presente la entidad financiera podrá ser un área, sector o persona- para el soporte, registro y seguimiento de los incidentes que surjan con los sistemas, la tecnología informática y los recursos asociados. De esta manera, se asegurará a los usuarios de los sistemas productivos, tanto internos como externos al centro de procesamiento de datos, que continuamente tengan disponibles y en correcto funcionamiento los recursos de sistemas de información y la tecnología asociada que los soporta.

Esta función deberá mantener un registro con los inconvenientes que hayan surgido (paradas de programa, fallos de sistemas, cancelación, fallas de hardware, y todo otro tipo de incidente relevante), cuyo detalle permita identificar el tipo de problema, el recurso afectado, el/los usuario/s involucrados, el tiempo de ocurrencia, la acción inmediata realizada, la derivación a los responsables, la resolución final de inconveniente, entre otros detalles que la entidad financiera estime registrar.

Esta documentación deberá ser mantenida como mínimo por 2 (dos) años, a efectos de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

6.1. Alcance.

Se encuentran alcanzadas las entidades financieras que intervengan en la prestación, por sí o por terceros en su nombre, de servicios financieros por intermedio de algunos de los siguientes Canales Electrónicos (CE), cuya definición y características se encuentra en el Glosario del punto 6.6.:

6.1.1. Cajeros Automáticos (ATM).

6.1.2. Terminales de Autoservicio (TAS).

6.1.3. Banca Móvil (BM).

6.1.4. Banca Telefónica (BT).

6.1.5. Banca por Internet (BI).

6.1.6. Puntos de Venta (POS).

6.1.7. Plataforma de Pagos Móviles (PPM)

6.2. Procesos de referencia.

De modo referencial y con el objetivo de facilitar la implementación de los requisitos de seguridad determinados en esta sección, la Gestión de Seguridad de los Canales Electrónicos se entiende como el ciclo de procesos que reúnen distintas tareas, especialidades y funciones, de manera integrada e interrelacionada, repetible y constante para la administración, planificación, control y mejora continua de la seguridad informática en los Canales Electrónicos.

Los Procesos de Referencia aquí señalados, reúnen el conjunto de tareas y especialidades que las entidades pueden poseer, con estas u otras denominaciones y en la composición orgánica que mejor atienda sus intereses y satisfaga las funcionalidades y propósitos descriptos. Asimismo, deben informar a la Gerencia de Auditoría Externa de Sistemas la estructura e interrelaciones orgánicas y operativas que en sus organizaciones se corresponda:

6.2.1. Concientización y Capacitación (CC).

Proceso relacionado con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para el desarrollo de tareas preventivas, detectivas y correctivas de los incidentes de seguridad en los Canales Electrónicos.

6.2.2. Control de Acceso (CA).

Proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los Canales Electrónicos.

6.2.3. Integridad y Registro (IR).

Proceso destinado a la utilización de técnicas de control de la integridad y registro de los datos y las transacciones, así como el manejo de información sensible de los Canales Electrónicos y las técnicas que brinden trazabilidad y permitan su verificación. Incluye, pero no se limita a transacciones, registros de auditoría y esquemas de validación.

6.2.4. Monitoreo y Control (MC).

Proceso relacionado con la recolección, análisis y control de eventos ante fallas, indisponibilidad, intrusiones y otras situaciones que afecten los servicios ofrecidos por los Canales Electrónicos, y que puedan generar un daño eventual sobre la infraestructura y la información.

6.2.5. Gestión de Incidentes (GI).

Proceso relacionado con el tratamiento de los eventos y consecuentes incidentes de seguridad en Canales Electrónicos, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

6.3. Requisitos generales.

Complementariamente a los requisitos técnico-operativos que se indiquen, las entidades financieras, deben satisfacer los siguientes requisitos generales con independencia de la naturaleza, composición y estructura de los servicios que presten por medio de sus Canales Electrónicos.

6.3.1. De la Matriz de Escenarios y la Gestión de Riesgo Operacional de Tecnología.

6.3.1.1. Deben encuadrar la operatoria de los Canales Electrónicos que gestionen, dentro de los escenarios comprendidos en la Matriz de Escenarios del punto 6.5., implementando cómo mínimo y según la criticidad que se establezca, los requisitos indicados para cada escenario aplicable.

6.3.1.2. Atento a las normas sobre “Lineamientos para la Gestión de Riesgos en las Entidades Financieras”, las entidades deben incluir en su análisis de riesgo operacional, todos los activos informáticos relacionados con los escenarios aplicables, estableciendo un nivel de criticidad equivalente al indicado por este Banco Central para cada escenario o cuando no esté indicado, por lo establecido en el punto 6.4.2.

6.3.1.3. Lo indicado en el punto 6.3.1.2., debe encontrarse documentado y formar parte de la metodología de gestión de riesgos operacionales de la entidad financiera. A su vez, es complementario de los análisis de riesgo periódicos y los mecanismos de seguridad informática implementados para minimizar los riesgos detectados.

6.3.1.4. Los errores de encuadramiento detectados por las auditorías internas y/o externas obligan a las entidades a efectuar los ajustes correspondientes en un plazo no mayor a 180 días corridos posteriores a su notificación, debiendo presentar a la Superintendencia de Entidades Financieras y Cambiarias, un informe de las adecuaciones efectuadas avalado por una verificación de conformidad de su Auditoría Interna, posterior al vencimiento de plazo indicado. La Superintendencia de Entidades Financieras y Cambiarias podrá realizar una verificación de lo actuado

6.3.2. Del cumplimiento de los requisitos técnico-operativos mínimos.

6.3.2.1. Las entidades deben desarrollar, planificar y ejecutar un plan de protección de sus activos, procesos, recursos técnicos y humanos relacionados con los Canales Electrónicos bajo su responsabilidad, basado en un análisis de riesgo de actualización periódica mínima anual, en su correspondencia con la Matriz de Escenarios y en los requisitos técnico-operativos detallados en los puntos 6.7. y subsiguientes.

6.3.2.2. Dentro de las tareas de gestión de la seguridad, e independientemente del área, personas o terceros que tengan a su cargo la función y la ejecución de las tareas, las entidades deben contar con funciones y tareas relacionadas con los siguientes procesos estratégicos de seguridad para sus Canales Electrónicos:

6.3.2.2.1. Concientización y Capacitación. Complementariamente a lo indicado en el punto 6.2.1., las entidades deben contar con un programa de concientización y capacitación de seguridad informática anual, medible y verificable, cuyos contenidos contemplen todas las necesidades internas y externas en el uso, conocimiento, prevención y denuncia de incidentes, escalamiento y responsabilidad de los Canales Electrónicos con los que cuentan.

6.3.2.2.2. Control de Acceso. Complementariamente a lo previsto en el punto 6.2.2., las entidades deben adquirir, desarrollar y/o adecuar los mecanismos implementados para la verificación de la identidad y privilegios de los usuarios internos y externos, estableciendo una estrategia basada en la interoperabilidad del sistema financiero, la reducción de la complejidad de uso y la maximización de la protección del usuario de servicios financieros.

6.3.2.2.3. Integridad y Registro. Complementariamente a lo indicado en el punto 6.2.3., las entidades deben garantizar un registro y trazabilidad completa de las actividades de los Canales Electrónicos en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación.

6.3.2.2.4. Monitoreo y Control. Complementariamente a lo previsto en el punto 6.2.4 las entidades deben contar con recursos técnicos y humanos dispuestos para asegurar un control permanente y continuo de todos sus Canales Electrónicos y una clasificación de los eventos registrables, así como patrones de búsqueda y correlación.

6.3.2.2.5. Gestión de Incidentes. Complementariamente a lo indicado en el punto 6.2.5., las entidades deben arbitrar los esfuerzos necesarios para contar en sus organizaciones o a través de terceros bajo coordinación y control propio, con equipos de trabajo especializado en la atención, diagnóstico, análisis, contención, resolución, escalamiento e informe de los incidentes de seguridad de todos sus Canales Electrónicos, de manera formal e integrada.

6.3.3. De la responsabilidad sobre los Canales Electrónicos.

6.3.3.1. El Directorio o autoridad equivalente de la entidad, es el responsable primario de la gestión de seguridad informática de la operatoria de los Canales Electrónicos desde el primer momento en que sus clientes se suscriben a los servicios ofrecidos por su intermedio o reciben medios de pago emitidos por ellas o en su nombre para su uso dentro de los alcances establecidos en el acuerdo de prestación.

6.3.3.2. La responsabilidad de las entidades financieras en los servicios y operaciones cursadas por medio de Canales Electrónicos incluye, pero no se limita a los medios operativos, físicos y lógicos de acceso e intercambio de información con los usuarios, la infraestructura de procesamiento, transporte y custodia de información operativa y financiera. Excluye aquellos medios físicos o lógicos propiedad y tenencia exclusiva de los clientes, siempre que admitan limitar su uso y disponibilidad a la compatibilidad con los mecanismos necesarios para brindar un servicio bancario seguro.

6.3.3.3. Las empresas prestadoras de servicios de procesamiento, transporte, custodia y/o tareas o procesos de seguridad informática relacionados con los Canales Electrónicos de las entidades financieras, incluyendo a los propietarios de licencias o marcas que por acuerdo con las entidades financieras facilitan el uso de sus recursos e infraestructura, se encuentran alcanzadas por las condiciones establecidas en la Sección 7., en la Circular CREFI - 2, Capítulo II, Sección 6. y en otras regulaciones técnicas complementarias.

6.3.3.4. Las entidades financieras deben establecer e informar a este Banco Central la estructura orgánica dispuesta y la nómina de responsables de las tareas relacionadas con los Procesos de Referencia indicados en el punto 6.2. e informar de cualquier novedad o cambio efectuado a la misma en un plazo no mayor a 10 días hábiles luego de ocurrido el hecho. Esta información incluye: los procesos, tareas y responsables en empresas prestadoras dónde se encuentre descentralizada parte o la totalidad de los servicios de Canales Electrónicos.

6.3.3.5. Las propuestas de implementación de un nuevo CE o modalidad diferente de las contempladas en esta sección, previo un análisis de riesgo de la entidad financiera, deben ser informadas al menos con 60 días de anticipación a la Gerencia Principal de Seguridad de la Información, para que en conjunto con la Gerencia Principal de Sistemas de Pago y Cuentas Corrientes analicen los alcances particulares, características técnicas e impacto de la implementación y de corresponder brinden las eventuales recomendaciones que consideren necesarias o realicen los ajustes normativos que correspondiesen.

6.3.3.6. En todos aquellos casos en que la operación no esté asociada a una clave de identificación personal, ante el desconocimiento por parte del cliente de una transacción efectuada mediante POS o PPM, las entidades financieras deben proceder a la inmediata devolución/acreditación de los fondos al cliente, sin perjuicio de iniciar la investigación de la operación y eventualmente, las acciones administrativas y/o legales que correspondieran.

6.4. Escenarios de Canales Electrónicos.

6.4.1. Guía.

Cada escenario está compuesto por: una categoría de agrupación temática, una situación considerada dentro de la categoría, una determinación de la aplicabilidad del escenario en los Canales Electrónicos considerados, un valor de criticidad que indica la importancia relativa del escenario y que afecta los requisitos mínimos considerados y, finalmente, un conjunto de requisitos técnico-operativos para controlar la situación descripta.

Un escenario se presenta como una fila dentro de la matriz. Se utilizan tres categorías, que agrupan los principales escenarios de interés:

- Credenciales y Medios de Pago (CM). Se refiere a los elementos dispuestos para la identificación, autenticación y autorización de acceso/uso de los medios y dispositivos de los Canales Electrónicos. Se incluyen aquellos elementos físicos y lógicos que funcionan como mecanismos de consumo, sustitutos del efectivo, que permiten generar transacciones financieras de débito o crédito en las cuentas de los clientes.
- Dispositivo/Aplicación (DA). Se refiere a las características de los dispositivos y piezas físicas y lógicas intervinientes en la operación de los Canales Electrónicos respectivos.
- Transacciones (TR). Se refiere a la naturaleza de las operaciones financieras, operativas y de consulta que permita realizar el Canal Electrónico.

Las situaciones describen el escenario particular sujeto a tratamiento y para el que se han determinado requisitos técnico-operativos mínimos particulares.

La aplicabilidad se encuentra determinada para los Canales Electrónicos considerados en la norma y en el escenario en particular. No a todos los canales les aplica el mismo escenario descripto.

6.4.2. Criticidad y Cumplimiento.

La criticidad es un ponderador que establece el nivel de importancia relativo de un escenario y sus necesidades regulatorias. Las entidades deben instrumentar los mecanismos necesarios para considerar la aplicabilidad del escenario a su contexto particular y su inclusión en la matriz de riesgo operacional de tecnología que emplee en su gestión de riesgo operacional acorde con lo indicado en los puntos 6.4.1. y subsecuentes.

El nivel de obligación de las entidades de cumplir los requisitos técnico-operativos está determinado por tres elementos: la criticidad asignada, la vigencia determinada en cada requisito técnico-operativo y los resultados de la gestión de riesgo de las entidades financieras.

Los valores de criticidad, los criterios utilizados para su asignación a cada escenario y el cumplimiento se determinan según lo indicado en la siguiente tabla.

Valor	Descripción	Criterios de asignación	Cumplimiento
1	Alta exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma extendida la disponibilidad de los servicios y la confiabilidad de el/los CE, la entidad financiera y el sistema financiero en general.	• Exposición al riesgo sistémico y propagación del efecto negativo. • Impacto económico sobre los clientes y la entidad financiera. • Nivel de penetración del Canal Electrónico y Medio de Pago asociado. • Interoperabilidad y efectos sobre otros CE.	Obligatorio. Las entidades financieras deben satisfacer los requisitos técnico operativos de cada escenario de acuerdo con la Tabla de Requisitos correspondiente (punto 6.7).
2	Moderada exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad de el/los CE involucrados, la entidad financiera y el sistema financiero en general.		Alineado. Las entidades deben realizar sus mejores esfuerzos para satisfacer los requisitos técnico-operativos de cada escenario, implementando medidas compensatorias y/o alternativas en aquellos requisitos que no satisfagan los indicados en la Tabla de Requisitos correspondiente (punto 6.7).
3	Baja exposición al riesgo cuya falta o deficiencia de tratamiento afecta de forma limitada la disponibilidad y la confiabilidad en el/los CE involucrados, la entidad financiera o el sistema financiero en general.		Esperado. Las entidades podrán satisfacer los requisitos de acuerdo con los resultados formales de su gestión de riesgo

La asignación de los valores en cada escenario, es una potestad de este Banco Central. No obstante, cuando no se encuentre asignado un valor a un determinado escenario, las entidades financieras deben asignarlo siguiendo los criterios establecidos en la tabla y los resultados formales de su gestión de riesgo operacional. Este Banco Central queda facultado para realizar actualizaciones periódicas de estos valores, adecuando los mismos de acuerdo con el resultado de sus verificaciones, el comportamiento del sistema financiero y el contexto nacional.

6.5. Matriz de Escenarios.

Matriz de Escenarios					
Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Credenciales y Medios de Pago	ECM001	Generación, distribución y descarte de credenciales que incluyen TC/TD.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA015; RCA016; RCA017; RCA018; RCA019; RCA020; RCA021; RCA031; RCA037; RCA038; RCA043; RCA044; RCA045; RIR002; RIR003; RIR005; RIR009; RGI001; RGI002; RGI003 y RGI005.
	ECM002	Generación, distribución y descarte de Credenciales que no incluyen TC/TD.	BI; BM; PPM y BT.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC010; RCC013; RCC014; RCA001; RCA003; RCA009; RCA011; RCA012; RCA014; RCA016; RCA017; RCA018; RCA019; RCA028; RCA029; RCA037; RCA043; RIR002; RIR003; RIR005; RIR009; RGI001, RGI002; RGI003 y RGI005.
	ECM003	Suscripción, presentación, uso, renovación y baja de credenciales que incluyen TD/TC.	ATM; TAS; PPM y POS.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA006; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA013; RCA015; RCA017; RCA018; RCA022; RCA023; RCA025; RCA026; RCA030; RCA031; RCA036; RCA040; RCA041; RCA044; RCA045; RCA048; RIR001; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR015; RIR016; RMC005; RMC006; RMC007; RMC008; RMC009; RMC010; RGI001, RGI002; RGI003 y RGI005.
	ECM004	Suscripción, presentación, uso, renovación y baja de credenciales sin TD/TC.	BI; BM; PPM; TAS y BT.	**1**	RCC001; RCC002; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCC014; RCA002; RCA003; RCA004; RCA005; RCA007; RCA008; RCA009; RCA010; RCA011; RCA012; RCA014; RCA017; RCA018; RCA022; RCA023; RCA024; RCA026; RCA027; RCA028; RCA030; RCA039; RCA040; RCA041; RCA042; RIR001; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR015; RIR016; RMC001; RMC005; RMC006; RMC008; RMC010; RGI001, RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)

Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Dispositivos/Aplicaciones	EDA001	Diseño, funcionalidad y homologación de dispositivos suministrados por la entidad o el operador.	ATM; POS y TAS.		RCC006; RCC012; RCC010; RCC013; RCA020; RCA033; RCA034; RCA036; RCA037; RCA038; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010 y RIR011.
	EDA002	Compatabilización de dispositivos propios del usuario.	BI; BT; PPM y BM.	**2**	RCC006; RCC010; RCC011; RCC013; RCA034; RCA035; RCA037; RIR012; RIR017 y RIR019.
	EDA003	Diseño, funcionalidad y homologación de aplicaciones para la interacción del usuario con el CE, suministrados por la entidad/operador.	BI; BT; PPM y BM.		RCC006; RCC010; RCC012; RCC013; RCA027; RCA033; RCA034; RCA037; RIR001; RIR002; RIR003; RIR004; RIR005; RIR009; RIR010; RIR011; RIR012 y RIR017.
	EDA004	Operaciones y mantenimiento de dispositivos/aplicaciones con manejo físico de valores.	ATM; TAS y POS.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA015; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR010; RIR014; RIR015; RIR018; RMC003; RMC006; RMC007; RMC009; RMC010; RMC012; RMC013; RGI001; RGI002; RGI003 y RGI005.
	EDA005	Operaciones y mantenimiento de dispositivos/aplicaciones sin manejo físico de valores.	BI; BT; PPM y BM.		RCC001; RCC005; RCC006; RCC007; RCC008; RCC009; RCC010; RCC012; RCC013; RCA012; RCA013; RCA014; RCA018; RCA023; RCA026; RCA033; RCA037; RCA040; RIR002; RIR003; RIR004; RIR005; RIR007; RIR009; RIR010; RIR014; RIR015; RMC001; RMC003; RMC006; RGI001; RGI002; RGI003 y RGI005.

Matriz de Escenarios (continuación)

Categoría	Escenario	Situación	Aplicabilidad	Criticidad	Requisitos
Transacciones	ETR001	Depósito de valores físicos en el CE con destino directo a cuentas bancarias o pagos de bienes y servicios.	ATM y TAS.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR002	Extracción de efectivo por CE.	ATM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC013; RCA032; RCA040; RCA046; RCA047 RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR003	Pago de bienes o servicios.	ATM; TAS; POS; BI; BM; PPM y BT.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR004	Transferencias de fondos entre cuentas de un mismo titular y misma entidad financiera.	ATM; TAS; BI; BM y BT.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR005	Transferencias Inmediatas.	ATM ; BM y BI.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR006	Transferencias ordinarias	ATM; TAS; BI y BM.	**1**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR007	Solicitud, formalización y acreditación de operaciones de crédito.	ATM; TAS; BI y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032; RCA040; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR008	Transacciones de consulta, instrucción operativa o instrucción financiera con confirmación por vía tradicional.	ATM; TAS; BI; BT y BM.		RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR014; RIR015; RIR016; RMC001; RMC006; RMC008; RMC009; RGI001; RGI002; RGI003 y RGI005.
	ETR009	Nuevas operatorias transaccionales no contempladas en otros escenarios, con o sin movimiento de fondos.	ATM; TAS; POS; BI; BT; PPM y BM.	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA032, RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003 y RGI005.
	ETR010	Transacciones de Bajo Valor: extracciones de efectivo, pago de bienes y/o servicios y transferencias inmediatas.	ATM; POS; BI; BM y PPM	**2**	RCC001; RCC002; RCC003; RCC004; RCC005; RCC006; RCC007; RCC008; RCC009; RCC011; RCC013; RCA040; RCA046; RCA047; RIR002; RIR003; RIR004; RIR005; RIR006; RIR007; RIR008; RIR009; RIR013; RIR014; RIR015; RIR016; RMC001; RMC002; RMC004; RMC005; RMC006; RMC008; RMC009; RMC011; RGI001; RGI002; RGI003; RGI005.

6.6. Glosario de términos utilizados en la Sección 6.

Se incluye, en orden alfabético, la definición aplicable a los términos y acrónimos utilizados en esta sección con objeto de facilitar la interpretación y ofrecer mayor claridad a los contenidos.

Activo. Comprende a los recursos, personas y medios indispensables para la ejecución de uno o más procesos de negocios que sean relevantes en los resultados esperados de estos últimos.

Autenticación Fuerte - Doble Factor. Comprende la utilización combinada de dos factores de autenticación, es decir dos elementos de las credenciales de distinto factor. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación** y **Credenciales**.

Banca Electrónica. Comprende a todo servicio bancario y/o financiero, ofrecido por una entidad y basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros, con mínima o ninguna asistencia o participación de un operador humano. La Banca Electrónica incluye pero no se limita a la implementación de Canales Electrónicos con las características indicadas en esta norma.

Banca Móvil (BM). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de aplicaciones (programas) informáticas diseñadas para su implementación y operación en dispositivos móviles propios del usuario, que vinculan al dispositivo, la aplicación y las credenciales del cliente de manera única con una plataforma de servicios financieros, en un centro de procesamiento de la entidad (propio o de un tercero) y se comunican, mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de voz y datos bajo administración de un operador público o privado.

Banca por Internet (BI). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de programas informáticos diseñados para su operación mediante el acceso a sitios publicados en Internet, bajo administración de una entidad u operador y el uso de motores de navegación instalados en dispositivos propios del usuario, que se comunican con un centro de procesamiento de la entidad (propio o de un tercero) mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de datos bajo administración de un operador público o privado.

Banca Telefónica (BT). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de programas informáticos diseñados para su operación con teléfonos propiedad o no del consumidor financiero y que se comunican con un centro de procesamiento de la entidad (propio o de un tercero) mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de voz y datos bajo administración de un operador público o privado.

Cajeros Automáticos (ATM). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de los dispositivos conocidos cómo Cajeros Automáticos o ATM ("Automated Teller Machine") en sus distintas modalidades: Dispensadores de Efectivo, Kioscos Digitales, entre otros y que permitan por lo menos, la extracción de efectivo sin intervención de un operador humano.

Canales Electrónicos (CE). Comprende a los medios, dispositivos, redes y servicios informáticos dispuestos por las entidades financieras, por sí o por intermedio de terceros en calidad de prestadores asociados, para la instrucción de operaciones bancarias, con efecto sobre las cuentas de uno o más usuarios de servicios financieros y/o clientes de esas entidades.

Cliente - usuario de servicios financieros - usuario. Los términos "cliente" y "usuario de servicios financieros" son equivalentes y se refieren a la persona física o jurídica que se encuentra identificada y suscrita a los servicios de una o más entidades financieras. El término "usuario" es una denominación genérica aplicable a clientes y no clientes.

Contramedidas. Comprende a todas las acciones, planes, tareas operativas, mecanismos de software o hardware dispuestos para mitigar el riesgo de ocurrencia de ataque o compromiso de una vulnerabilidad conocida.

Contraseña. Elemento de las credenciales basado en una pieza de información compuesta por una secuencia de caracteres o símbolos sólo conocidos por el usuario tenedor (factor basado en "algo que sabe") o generados por dispositivo (factor basado en "algo que tiene").

Control dual. Comprende al proceso que utiliza dos o más participantes de forma separada (individuos, organizaciones, entre otros), quienes operan en forma concertada para proteger funciones o información de carácter confidencial, asegurando que ningún participante podrá llevar adelante la función sin la intervención del resto de los participantes.

Credenciales. Comprende a todos los elementos físicos o lógicos provistos por la entidad/operador, necesarios para algunas o todas las siguientes acciones durante el uso de un Canal Electrónico específico: presentación/identificación, autenticación, solicitud, verificación, confirmación/autorización. Complementariamente, considérese lo expuesto sobre **Factores de Autenticación**.

Datos personales públicos. Comprende a datos de personas físicas que pueden obtenerse de fuentes públicas, tales como nombres y apellidos, fechas de nacimiento, números de identificación nacional y laboral, entre otros.

Dispositivos. Comprende a los elementos físicos específicamente diseñados y dispuestos para la interacción directa entre los clientes y el Canal Electrónico, así como otros usuarios calificados para el mantenimiento y control en sitio. Incluye los elementos lógicos y/o aplicaciones necesarios para brindar funcionalidad y operación a los elementos físicos.

Encripción - métodos. Comprende a los métodos para el cifrado de información con el propósito lograr confidencialidad de su contenido y limitar su revelación a la aplicación de un mecanismo de descifrado previsto. Algunos métodos considerados en esta norma, incluyen, pero no se limitan a DES ("Data Encryption Standard"), 3DES (triple cifrado del DES), entre otros.

Escalamiento - Escalamiento de incidentes. Comprende al protocolo formal y procedimientos específicos para el flujo de ejecución e informe de las actividades de recepción, diagnóstico, análisis, contención, corrección y reporte de los incidentes de seguridad en los Canales Electrónicos.

Evento de seguridad. Comprende al hecho ocurrido e identificado sobre el estado de un sistema, servicio o red que indique un desvío de la política de seguridad establecida, una falla de las medidas de seguridad implementadas o una situación desconocida previamente que pueda ser relevante a la seguridad.

Factores de Autenticación. Las credenciales utilizadas en los CE pueden ser del siguiente tipo o factor: "algo que sabe", (Contraseña, dato personal, entre otros), "algo que tiene" (Tarjeta TC/TD, Token, entre otros), "algo que es" (Característica biométrica).

Identificación positiva. Comprende a los procesos de verificación y validación de la identidad que reducen la incertidumbre mediante el uso de técnicas complementarias a las habitualmente usadas en la presentación de credenciales o para la entrega o renovación de las mismas. Se incluyen pero no se limitan a las acciones relacionadas con: verificación de la identidad de manera personal, mediante firma holográfica y presentación de documento de identidad, mediante serie de preguntas desafío de contexto variable, entre otros.

Incidente de seguridad en Canales Electrónicos. Se conforma por el evento o serie de eventos de seguridad, operativos y tecnológicos interrelacionados que generen una exposición no deseada o esperada de las credenciales, transacciones, datos de los clientes y el servicio bancario asociado y que posean una probabilidad significativa de comprometer las operaciones y amenazar la seguridad informática.

Infraestructura de redes. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y transporte de voz y datos que interconectan e integran los recursos de la infraestructura de tecnología y sistemas.

Infraestructura de seguridad. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y control de la plataforma tecnológica asociada a la seguridad de los Canales Electrónicos.

Infraestructura de tecnología y sistemas. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento, procesamiento y control de los servicios de tecnología informática asociada a los Canales Electrónicos.

Journal o Tira de auditoría. Comprende a los mecanismos físicos y/o lógicos dispuestos para el registro de la actividad de los dispositivos de los Canales Electrónicos asociados al acceso a los servicios e instrucción de operaciones.

Kiosco digital. Comprende a los dispositivos con emplazamiento y características físicas similares a los ATM ("Automated Teller Machine") que prestan una gama de servicios mayor a la dispuesta para estos, incluyendo pero no limitándose a los servicios ofrecidos por los TAS.

Medios de Pago en Canales Electrónicos. Comprende a los medios o elementos físicos o electrónicos representativos y útiles para la concertación de operaciones financieras en Canales Electrónicos, que incluyen, pero no se limitan a: tarjetas de pago, débito o crédito.

Operaciones "en línea" o "fuera de línea". La operatoria "en línea" ocurre cuando la actividad del servicio o canal electrónico se encuentra en estado activo sincrónico entre los distintos puntos de autorización y respuesta, el dispositivo y el operador y/o entidad financiera, siendo que en cada transacción se perfeccionan la validación, autenticación y confirmación de credenciales y transacciones financieras. La operatoria "fuera de línea" ocurre cuando la actividad del servicio o canal electrónico se encuentra en estado asincrónico entre los distintos puntos de resolución de autorización y respuesta, siendo necesario el perfeccionamiento de la validación, autenticación y confirmación de credenciales independientemente del momento de la validación, autenticación y confirmación de la transacción financiera.

Operadores. Se utiliza el término en forma indistinta para indicar a las empresas prestadoras de servicios financieros dentro de los indicados en esta sección, que cuenten con un acuerdo de servicio con las entidades financieras o actúen en su nombre o cuyas operaciones afecten las cuentas de crédito y/o depósito de sus clientes.

Plataforma de Pagos Móviles (PPM). Aplicación o servicio informático para todo tipo de dispositivos móviles y computadores personales propios del usuario, que permite la asociación de tarjetas bancarias vinculadas a su vez a cuentas de crédito o débito, sin límite de número, entidades u operadores, para la instrucción de pagos y transferencias mediante crédito a cuentas de terceros adheridos o transferencias inmediatas en cuentas a la vista con acuerdo de las entidades financieras y operadores de transacciones financieras del Sistema Financiero Nacional

Punto de compromiso. Comprende al individuo, empresa o comercio adquirente de POS en el que se detecta un patrón similar de operaciones sospechosas o fraudulentas con TD/TC.

Puntos de venta (POS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al consumidor financiero, que se basan en la utilización de distintos medios de pago electrónico (Tarjetas de Débito/Crédito) para el pago de servicios u operaciones financieras que generen un débito o un crédito en las cuentas bancarias que el cliente posee con el emisor y que confirman tales operaciones mediante la comunicación local o remota con un centro de procesamiento de la entidad emisora o tercero interesado con acuerdo previo del emisor, mediante redes públicas de comunicación aptas y aprobadas por autoridad competente para la transmisión de datos bajo administración de un operador público o privado.

Redes privadas y públicas. Infraestructura de comunicaciones se considera privada cuando es administrada por una entidad financiera o un tercero en su nombre y accesible de forma exclusiva y única para la infraestructura de tecnología y sistemas de la entidad financiera. Se considera pública cuando la infraestructura de comunicaciones es administrada por un operador independiente y accesible mediante suscripción previa a múltiples empresas o individuos.

Servicios Financieros. Incluye la prestación de operaciones bancarias, cambiarias y/o financieras, de instrucción legal por medio bancario o pago de bienes y servicios.

Sesión en Canales Electrónicos. Comprende al período durante el cual un consumidor financiero (persona o comercio) puede llevar a cabo transacciones financieras, operativas o consultas permitidas en un Canal Electrónico. Se entenderá compuestos por las siguientes etapas: ***Presentación*** (Ingreso de Credenciales, también referido como *Inicio de Sesión*), ***Autenticación*** (Validación y autenticación de los valores de las credenciales ingresados), ***Solicitud*** (Selección de la opción o transacción elegida por la persona/comercio y la composición del mensaje correspondiente), ***Verificación*** (Etapa alternativa para la verificación de la identidad y reválida de credenciales ante determinado tipo o características de la transacción elegida), ***Confirmación*** (Validación y autorización de la transacción y cierre de ciclo). Las etapas mencionadas son consecutivas con excepción de la etapa de Autenticación, que puede ocurrir continuando la etapa de solicitud y antes de la etapa de Verificación.

Tarjetas de Débito/Crédito (TD/TC). Comprende a elementos asociados a las credenciales de acceso a algunos Canales Electrónicos, habitualmente basados en piezas plásticas cuyas inscripciones y características físicas las hacen aptas para su presentación y lectura en dispositivos de autenticación y autorización de los mismos. En la presente norma se mencionan en dos modalidades habituales de uso, como medios primarios de transacciones comerciales de crédito/débito o como medios primarios de acceso a operaciones financieras por ATM ("Automated Teller Machine").

Telefonía fija. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía fija o terrestre autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere una suscripción personal o comercial con locación del servicio en domicilio específico.

Telefonía móvil. Servicios de comunicación ofrecidos por empresas de telecomunicaciones que utilizan los espectros de telefonía móvil autorizados a nivel nacional, y que incluyen los servicios de enlace e intercambio de voz y datos. Requiere suscripción personal o comercial pero es independiente de la locación del suscriptor.

Terminales de autoservicio (TAS). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio al cliente bancario, que se basan en la utilización de los dispositivos conocidos como Terminales de Autoservicio u otros de similar naturaleza, enlazados a la red institucional de la entidad responsable, ya sea por conexión directa o indirecta (sucursal, proveedor) a un centro de procesamiento y que permitan por lo menos el depósito y transferencia de fondos y excluyan la extracción de efectivo sin intervención de un operador humano.

Transacciones de Bajo Valor. Transacciones financieras por medio de Canales Electrónicos habilitados hasta el máximo establecido en la Comunicación "A" 5982 y sus modificatorias.

6.7. Tablas de requisitos técnico-operativos.

6.7.1. Tabla de requisitos de Concientización y Capacitación.

Tabla de requisitos de Concientización y Capacitación		
Código de requisito	**Descripción de requisito**	**Alcance**
RCC001	Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.	
RCC002	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo "ingeniería social", "phishing", "vishing" y otros de similares características.	
RCC003	Los contenidos del programa de CC deben incluir: técnicas de detección y prevención del "skimming" y apropiación de datos de las credenciales mediante técnicas de intervención física.	
RCC004	Los contenidos del programa de CC deben incluir: técnicas de detección de situaciones sospechosas en el recinto o entorno de acceso al CE.	
RCC005	Mantener informado al personal interno, personal responsable por la gestión del CE, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descripto.	
RCC006	Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante. b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario. c. Orientado pero no limitado a: personal interno, personal responsable por la gestión del CE, proveedores y clientes.	
RCC007	Con una periodicidad mínima anual, debe efectuarse un análisis del Programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC. b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.	
RCC008	Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.	
RCC009	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre el uso seguro de los dispositivos propios del usuario y los dispositivos provistos por la entidad/operador.	
RCC010	Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de CE.	
RCC011	Los contenidos del programa de CC deben incluir: acciones específicas del usuario para la configuración de los dispositivos propios para comunicación con el CE (teléfonos, computadores personales, tabletas electrónicas, entre otros). Incluye pero no se limita a las características diferenciadas por dispositivo para el almacenamiento de datos, reposo/bloqueo automático, eliminación de información antes del descarte o reemplazo del dispositivo, actualización de sistemas operativos y piezas de software provistas por la entidad para uso del CE.	
RCC012	Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los dispositivos y piezas de software provisto por la entidad/operador, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.	

Tabla de requisitos de Concientización y Capacitación (continuación)

Código de requisito	Descripción de requisito	Alcance
RCC013	Las entidades/operadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación que asegure: a. Que los destinatarios se encuentran continuamente informados. b. Que los destinatarios pueden efectuar consultas y evacuar dudas.	
RCC014	En la selección/cambio, por parte del cliente, de los valores de los elementos de autenticación basados en el factor “algo que sabe”, la entidad/operador deben recomendar al titular que los valores no se compongan al menos de: a. Una secuencia de número asociado a un dato personal público. b. Serie de caracteres o números iguales. c. Incremento o decremento de número consecutivo. d. Fechas de significación histórica.	

6.7.2. Tabla de requisitos de Control de Acceso.

Tabla de requisitos de Control de Acceso		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA001	Los procesos de distribución de elementos de identificación y autenticación basados en el factor "algo que sabe" deben ser siempre separados de la distribución de los elementos basados en el factor "algo que tiene".	
RCA002	La renovación de factores de identificación y autenticación basados en "algo que sabe" debe permitir la autogestión del cliente bancario o la mínima intervención de un operador durante el proceso, asegurando que solamente el cliente conocerá los valores asignados.	
RCA003	Los elementos de autenticación basados en el factor "algo que sabe" no deben ser conocidos antes ni durante su generación y uso por los funcionarios, empleados, representantes o terceros vinculados con las actividades correspondientes al escenario.	
RCA004	El almacenamiento de valores correspondientes a los factores de autenticación de los clientes bancarios, sólo será permitido cuando estos se encuentren protegidos mediante técnicas que impidan su conocimiento a otros diferentes del cliente y sólo con propósitos de verificación automática de las credenciales presentadas por el cliente para acceder y/o confirmar operaciones en el CE.	
RCA005	Las habilitaciones y rehabilitaciones de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben ser efectuadas mediante un proceso que garantice la identificación positiva del titular (RCA040). Asimismo, estos elementos, sólo podrán estar vinculados durante su uso a una única persona de forma individual e intransferible.	
RCA006	En los dispositivos provistos por la entidad/operador que utilicen teclados físicos (PIN PAD) o teclados virtuales (imagen en pantalla) para el ingreso del factor basado en algo que sabe, el valor ingresado debe ser encriptado inmediatamente después de su ingreso mediante un algoritmo no menor a: a. 3DES para dispositivos que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. DES para dispositivos que permitan transacciones establecidas con criticidad de nivel distinto a 1 en los escenarios del punto 6.5.	A partir del 01/03/2013, es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA007	Los sistemas de acceso y verificación de credenciales de los CE contemplados en el escenario descripto, deben garantizar la no reutilización del último valor generado de los elementos de autenticación basados en el factor "algo que sabe" .	
RCA008	La caducidad de los elementos de autenticación basados en "algo que sabe", debe establecerse según el análisis de riesgo de cada entidad o al vencimiento del factor basado en "algo que tiene" asociado al canal, cuando aplique. No obstante, las entidades financieras deben implementar los mecanismos necesarios para que los clientes bancarios puedan voluntariamente realizar el cambio aún antes de ese plazo, así como prevenir su presentación luego de vencido el plazo que determina la validez de los mismos.	
RCA009	Los elementos de autenticación basados en el factor "algo que tiene", siempre que empleen mecanismos de autenticación dinámica (Token, tarjeta de coordenadas, entre otros), deben poseer al menos dos de las siguientes características: a. Mecanismos que impidan su duplicación o alteración (Anti tampering). b. Control de relación unívoca entre cliente/cuenta y dispositivo. c. Identificación única de fabricación. d. Recambio bianual.	
RCA010	Las entidades/operadores, deben aplicar técnicas de protección, según su análisis de riesgo que minimicen la exposición de los factores de identificación y autenticación basados en "algo que tiene", cuando los mismos sean presentados ante dispositivos o medios que revelen a terceros datos confidenciales o códigos de seguridad de las credenciales, en operatorias no presenciales (Internet, WebPos, Venta Telefónica, dispositivos desatendidos), considerando pero no limitándose a las siguientes técnicas: a. Uso de esquemas de verificación complementaria por vías seguras (segundo factor, secretos compartidos, técnicas consideradas en el requisito RCA040). b. Valores aleatorios de identificación de TD/TC (PAN o CVC/CVV variable).	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA011	Debe limitarse la exposición de los datos identificatorios de las credenciales a aquellos usuarios autorizados por la entidad/operador que por necesidades de uso/conocimiento se encuentren calificados para el acceso a esta información.	
RCA012	En la etapa de inicio de sesión/presentación de credenciales, las entidades/operadores, deben ejecutar acciones específicas para proteger la fortaleza de los factores de identificación y autenticación empleando optativamente: a. Dos factores de autenticación de distinto tipo (autenticación fuerte), en alguna de las combinaciones: "algo que tiene" y "algo que sabe", "algo que sabe" y "algo que es" o,"algo que tiene" y "algo que es". b. Dos factores de autenticación del mismo tipo (autenticación simple), dónde uno de ellos identifique de forma unívoca al usuario.	
RCA013	En caso de falla o indisponibilidad total o parcial de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el dispositivo provisto por la entidad/operador, debe mantenerse inhabilitado totalmente el mismo, informando y previniendo al usuario para que evite la presentación de credenciales y la recepción o entrega de valores.	
RCA014	Los elementos de autenticación basados en el factor "algo que sabe", utilizados en el CE, deben poseer una longitud no inferior a 8 caracteres para BI, 6 caracteres para BM y 4 caracteres para BT.	
RCA015	Los elementos de autenticación basados en el factor "algo que sabe" y sean estrictamente "numéricos" deben: a. Limitarse a elementos del tipo PIN ("Personal Identification Number"). b. Poseer una longitud mínima de 4 dígitos.	
RCA016	Durante todo el ciclo de las tareas asociadas al escenario, los datos y credenciales de un cliente no deben estar en posesión completa de una misma persona o grupo de personas o ser asociados a los datos del cliente salvo por los clientes mismos.	
RCA017	Los elementos de autenticación basados en el factor "algo que sabe" durante sus procesos de generación, uso y transporte deben encontrarse protegidos por medio de alguna de las siguientes técnicas: a. Encripción no menor a 3DES. b. Digesto irreversible o funciones de "hashing". En BT, cuando no se utilice alguna de las técnicas descriptas, se debe garantizar que el mecanismo de autenticación del factor sea distinto al empleado para otros CE de un mismo cliente y entidad financiera.	A partir del 01/03/2013 es aplicable a nuevas adquisiciones/desarrollos, reemplazos o actualizaciones de dispositivos/aplicaciones provistos por la entidad/operador.
RCA018	Los elementos de autenticación basados en el factor "algo que sabe" deben limitar su exposición durante el ingreso o reproducción, en los procesos de generación, renovación y uso, considerando, pero no restringiéndose a la implantación alternativa de: a. Máscaras visuales en la pantalla de dispositivos provistos por la entidad/operador. b. Teclados virtuales en aplicaciones provistas por la entidad/operador. c. Paneles protectores de visualización en los dispositivos provistos por la entidad/operador (ejemplo: PCI PIN - Security Requirement 2.0).	
RCA019	Los procesos de generación de los elementos de identificación y autenticación basados en el factor "algo que tiene" deben realizarse en un esquema de separación de funciones tal, que impida que se combinen con la generación de los elementos de identificación y autenticación basados en el factor "algo que sabe". Ejemplos: embozado de tarjetas y generación de PIN; la instancia de sincronización de un token está diferenciada de su distribución.	
RCA020	Los elementos de identificación y autenticación basados en TD/TC deben contar al menos con las siguientes características: a. Nombre y apellido del cliente bancario. b. Número interno de inscripción (número de tarjeta). c. Firma hológrafa o manuscrita. d. Fecha de vigencia. e. Fecha de vencimiento. f. Número de atención de denuncias.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA021	Los procesos de distribución de elementos de identificación y autenticación, basados en el factor "algo que tiene" deben garantizar la identificación positiva del titular antes de su entrega.	
RCA022	Los elementos de identificación y autenticación basados en el factor "algo que tiene", luego de su retención, deben tener una vigencia no mayor a 30 días hábiles para su descarte o desvinculación del cliente y sus cuentas en forma posterior al tiempo determinado en caso de no ser devueltos al cliente.	
RCA023	Los elementos de autenticación basados en el factor "algo que sabe" y "algo que es" deben bloquear el acceso al CE luego de no más de cinco intentos fallidos consecutivos de inicio de sesión, informar al usuario mediante el esquema implementado de alertas tempranas (RCA041) y aplicar un mecanismo de autenticación positiva para el desbloqueo dentro de los considerados en el requisito RCA040. Luego de un tiempo no mayor a 30 minutos desde el último intento fallido registrado, salvo casos de bloqueo, podrá reiniciarse el registro de intentos fallidos.	
RCA024	En caso de falla o indisponibilidad parcial o total de los mecanismos de seguridad (Control de Acceso, Monitoreo, Integridad y Registro) en el servicio provisto por y desde la entidad/operador, debe mantenerse inhabilitado totalmente el servicio, informando y advirtiendo al usuario para que evite la presentación de credenciales desde un dispositivo propio.	
RCA025	En los dispositivos provistos por la entidad/operador que acepten el ingreso (mecanismo de tracción) de TD/TC, y que por falla mecánica u olvido del usuario retuvieran una TD/TC en el dispositivo, la entidad/operador debe proceder a la devolución al titular de la TD/TC o en caso de no hacerse efectiva, a su destrucción en un tiempo no mayor a 10 días hábiles posteriores a su extracción en los procesos de balanceo o mantenimiento del dispositivo.	
RCA026	En todos los casos de factores de autenticación basados en "algo que sabe" que hayan sido generados por la entidad/operador, se deben implementar mecanismos para asegurar que el cliente bancario modifique los valores generados en su primera presentación ante el CE. Dicho cambio, puede efectuarse mediante un CE distinto del considerado en el escenario, siempre que utilice autenticación fuerte.	
RCA027	En todos los casos de factores de identificación de usuarios generados por la entidad/operador se debe ofrecer al usuario la posibilidad de modificar dicho valor a uno elegido por el usuario.	
RCA028	Los elementos de autenticación basados en el factor "algo que sabe", utilizados para el ingreso al CE, deben poseer una composición alfanumérica y una complejidad tal, que incluya al menos la combinación de tres de los siguientes atributos: a. Caracteres especiales. b. Letras mayúsculas. c. Letras minúsculas. d. Números. e. No contener más de dos caracteres alfanuméricos iguales y consecutivos. f. Estar compuestas por datos no triviales (se descartan: números de teléfono, nombres propios, entre otros). Solamente en los canales BM y BT podrán establecerse caracteres exclusivamente numéricos, con una complejidad tal que se prevenga la selección de: g. Serie de caracteres del mismo número. h. Incremento o decremento de número consecutivo.	
RCA029	Los elementos de autenticación de las credenciales basadas en el factor "algo que sabe" y empleados en el inicio de sesión del CE, deben prevenir estar asociadas a datos personales públicos del cliente bancario o de la entidad financiera.	
RCA030	La suscripción a un CE debe realizarse para su aprobación desde un medio que utilice identificación positiva de acuerdo con las técnicas descriptas en el requisito RCA040.	
RCA031	La generación y renovación del PIN asociado a una TD/TC basada en banda magnética según el RCA044 punto a, debe garantizar un valor diferente entre los canales ATM y POS, siempre que se utilice un PIN asociado a una misma TD/TC.	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA032	La entidad/operador debe ejecutar las siguientes acciones para la protección de las transacciones involucradas en el escenario: a. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, alguna de las técnicas descriptas en el requisito RCA012 punto a. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar técnicas de autenticación complementarias para revalidar la identidad del usuario autorizado, entre las que se incluyen pero no se limitan: secretos compartidos, mecanismos de autenticación simple, rellamada o uso de canal alternativo. b. En el caso de aplicar en la etapa de inicio de sesión/presentación de credenciales, la técnica descripta en el requisito RCA012 punto b. y antes de la confirmación de una transacción de banca individual o grupo interrelacionado de transacciones de banca comercial, debe aplicar alguna de las técnicas descriptas en el requisito RCA012 punto a. para revalidar la identidad del usuario autorizado entre las que se incluyen pero no se limitan: usb tokens, token con generación de contraseña o tarjetas de coordenadas. c. Posterior a la confirmación de la transacción y sólo cuando se superen patrones predeterminados en sus sistemas de monitoreo transaccional, debe aplicar al menos una de las técnicas descriptas en el requisito RCA040. Para el canal ATM, cuando se opere mediante uso de tarjeta con circuito integrado (CHIP) bajo estándar EMV y siempre que se satisfaga el cumplimiento del requisito RCA012 punto a, no será exigible el cumplimiento del punto a del requisito RCA032.	
RCA033	La información referida a mecanismos implementados por una entidad/operador para la seguridad del CE y que sea pieza esencial en la protección del mismo, debe conservarse protegido ante la exposición de su contenido a personas no autorizadas.	
RCA034	Los procesos de implementación, prueba y homologación de dispositivos provistos por la entidad/operador y/o aplicaciones específicas para dispositivos no provistos por la entidad/operador para el uso del CE, cuando lo requieran, sólo podrán utilizar credenciales bajo administración de la entidad/operador, no relacionadas con clientes bancarios y no habilitadas para entornos productivos.	
RCA035	Las piezas de software provistos por la entidad/operador para el uso del CE por medio de un dispositivo propio del cliente, no podrán comprometer la privacidad de estos ni de los datos del cliente contenidos en los mismos aun cuando medie autorización del cliente.	
RCA036	Los dispositivos provistos por la entidad/operador deben contar con características físicas que reduzcan la copia, obstrucción, visualización de terceros o retención ilegal de credenciales y valores monetarios, considerando pero no limitándose a la aplicación alternativa de: a. Detectores de objetos adosados a dispositivos provistos por la entidad/operador. b. Mecanismos de información explícita al usuario de las características del dispositivo provisto por la entidad/operador. c. Componentes anti-skimming en el ingreso de credenciales. d. Mecanismos de detección de apertura, violación o alteración de las condiciones físicas del dispositivo (“tampering detection”).	
RCA037	Deben estar descriptos los grupos, roles y responsabilidades para la administración lógica de los componentes de la red de servicios de cada CE.	
RCA038	Los elementos de identificación/autenticación basados en Tarjetas de Débito/Crédito, deben contar con las siguientes características de protección complementaria: a. Impresión de datos de la Tarjeta en bajo o sobre relieve u otra técnica que garantice la legibilidad de los datos identificatorios por al menos el tiempo de vigencia inscripto en la Tarjeta. b. Inclusión de hologramas, códigos de seguridad, entre otros. c. La identificación del emisor y de la entidad bancaria interviniente. d. Los medios de almacenamiento de datos en la Tarjeta (banda magnética, chip, entre otros), no deben almacenar datos completos o legibles de los factores de autenticación.	A partir del 01/03/2013 y sólo para renovaciones y nuevas TD/TC.

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA039	En un dispositivo/aplicación asociado a un CE en el que se utilice un mecanismo de autenticación dinámica (token, softtoken, tarjeta de coordenadas, entre otros) y que permita la ejecución de transacciones financieras consideradas en los escenarios con nivel de criticidad 1 de prefijo ETR, los valores generados para componer las "claves dinámicas", deben satisfacer cómo mínimo las siguientes características durante la petición, validación e ingreso de los valores solicitados: a. La clave dinámica debe poseer una estructura no menor a 4 dígitos numéricos aleatorios. b. Los valores de la clave dinámica generados en cada petición, deben tener una vigencia máxima de 120 segundos o hasta su autenticación, lo que ocurra primero. No se exigirá la vigencia por tiempo cuando la entidad/operador asegure que en la ejecución de transacciones financieras consideradas en los escenarios de prefijo ETR con nivel de criticidad 1, la sesión de un CE emplea un valor nuevo y diferente generado por el dispositivo de autenticación dinámica, tanto en la etapa de "inicio de sesión/presentación" como en la de "confirmación" durante una misma sesión. c. Los valores de la clave dinámica generados en cada petición, no deben ser conocidos antes de su generación y durante el proceso de ingreso y validación de los datos por otros individuos distintos del cliente bancario. d. Debe asegurarse una validación del valor generado que garantice su autenticidad estableciendo una correspondencia efectiva del valor generado en el dispositivo/aplicación con el resto de las credenciales del usuario que forman parte del proceso de autenticación. Por ejemplo mediante una sincronización temporal con los sistemas de autenticación del CE, o por comparación univoca de la semilla de generación. e. Las claves dinámicas tienen validez por única vez en una sola transacción de banca individual y un único grupo de transacciones interrelacionadas en la banca comercial. f. Los procesos de autenticación de la clave dinámica deben ocurrir en línea.	
RCA040	La identificación positiva incluye, pero no se restringe a la utilización combinada o no de las siguientes técnicas: a. Cuestionarios predefinidos con presentación aleatoria, con validación automática del sistema. b. Presentación de documentos de identidad emitidos por autoridad nacional que permitan la comparación y convalidación efectiva de las características del portador. c. Firmas holográficas comparables con registro electrónico. d. Identificación ante canal electrónico alternativo con doble factor de autenticación.	
RCA041	Las entidades/operadores deben poner a disposición de sus clientes la siguiente información, estableciendo mecanismos efectivos de alerta en un tiempo no mayor a 24 horas posteriores a la transacción/sesión y de acuerdo a las características de cada CE, sin perjuicio de incluir información adicional acorde con aquella generada por sus sistemas de monitoreo transaccional: a. Fecha y hora de la última transacción/sesión confirmada en el CE. b. Aviso de vencimiento de las credenciales con una antelación no menor al tiempo operativo necesario para su cambio/reposición. c. Nombres del usuario de la sesión y del titular de la cuenta accedida. d. Datos de contacto del servicio al cliente para reporte de irregularidades/consultas.	
RCA042	Las entidades/operadores deben asegurar que los enlaces/accesos desde sesiones de los CE a sitios no bancarios y/o servicios de un tercero que permitan el acceso y ejecución de transacciones bancarias consideradas en los escenarios del punto 6.5. con prefijo ETR, garanticen el cumplimiento de los mismos requisitos establecidos para el CE y no compartan datos confidenciales de las credenciales con los sitios y servicios del tercero.	
RCA043	Los elementos de identificación y autenticación basados en el factor "algo que tiene" luego de su generación y que permanezcan sin entrega efectiva a su destinatario por más de 90 días, deben: a. Descartarse o reasignarse a otro cliente bancario, en el caso de elementos de autenticación dinámica (tokens, tarjetas de coordenadas, entre otros). b. Descartarse en el caso de TD/TC.	

Tabla de requisitos de Control de Acceso (continuación)

Código de requisito	Descripción de requisito	Alcance
RCA044	Los elementos de identificación y autenticación basados en el factor "algo que tiene" deben contar con códigos de seguridad renovables, diferentes en cada renovación de TD/TC y aplicarse a las transacciones contempladas en los escenarios del punto 6.5. bajo prefijo ETR, de la siguiente forma: a. En TD/TC basadas en banda magnética, deben contar un código de verificación de la credencial no visible y almacenado en la banda (ejemplo: CVV1/CVC1) y un código de verificación de la transacción visible (ejemplo: CVV2/CVC2/CID) impreso en la TD/TC. Opcionalmente y sólo para transacciones cursadas de forma presencial (dispositivo físico POS) podrá sustituirse la implementación del código de seguridad de transacción visible en la TD/TC con algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031. b. En TD/TC basadas en el uso de circuito integrado (chip) o una combinación de este con otras técnicas, deben contar con un mecanismo de autenticación dinámica y un cifrado de los datos almacenados en el circuito integrado. Puede complementarse con un algún factor de autenticación del tipo "algo que sabe" o PIN en los términos del requisito RCA031.	
RCA045	Las entidades/operadores deben considerar, según sus análisis de riesgo, un reemplazo periódico de los elementos de identificación y autenticación basados en "algo que tiene, por nuevos elementos renovados en sus códigos de seguridad aplicando, por ejemplo, los siguientes criterios: a. Ante las siguientes situaciones presentadas por el tenedor: 1. Denuncia de robo, pérdida o deterioro. 2. Desconocimiento de transacciones efectuadas. b. Ante el vencimiento inscripto en un TD/TC con una antelación mínima de 20 días, deshabilitando en forma inmediata la emisión anterior o activación del reemplazo, lo que ocurra primero. c. Ante la detección de una de las situaciones consideradas en el requisito RMC009. d. Ante cambios de diseño, formato o técnicas de elaboración que modifiquen los elementos de seguridad de las TD/TC se debe proceder con un plan de reemplazo con ejecución no mayor al plazo restante para la renovación original. e. Ante la detección de fallas de fabricación o pérdida durante la distribución y/o almacenamiento. debe procederse al descarte, reemplazo y renovación de todas las TD/TC involucradas. Asimismo, las entidades deben considerar una migración paulatina de las TD/TC a tecnología de microcircuito integrado favoreciendo la expansión del mercado, la seguridad transaccional, la interoperabilidad y la evolución de los servicios financieros.	
RCA046	Las TD/TC basadas en circuito integrado (CHIP) según lo indicado en el requisito RCA044 y que además cuenten con banda magnética (Sistema Dual), no podrán formalizar transacciones mediante el uso de banda magnética cuando la terminal POS o ATM cuente con lector de CHIP habilitado salvo excepciones que deberán quedar con un registro diferenciado y formar parte de los análisis del punto RMC009.	

Tabla de requisitos de Control de Acceso (continuación)		
Código de requisito	**Descripción de requisito**	**Alcance**
RCA047	En la utilización de TD/TC basadas en circuito integrado (CHIP) bajo estándar EMV, y según el método de autenticación elegido, las entidades y operadores deben: a. Para TD/TC que utilicen el método de autenticación, basados en la verificación de en un dato estático o firma grabada en el CHIP (SDA -Static Data Authentication por sus siglas en Inglés) las transacciones de los escenarios del punto 6.5. bajo prefijo ETR sólo deberán realizarse en la modalidad "en línea" (ver glosario). Del mismo modo, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario) b. Para TD/TC que utilicen los métodos de autenticación basados en la generación dinámica de claves de autenticación (DDA/CDA – Dynamic Data Authentication/ Combined Dynamic Data Authenticacion), las transacciones de los escenarios del punto 6.5. bajo prefijo ETR podrán realizarse en las modalidades "en línea" o "fuera de línea". Por otra parte, deberán incorporar un segundo factor de autenticación de acuerdo a lo indicado en el requisito RCA032 cuando las transacciones involucren extracciones, transferencias o pagos de bienes y servicios fuera de los límites del concepto "bajo valor" (ver glosario)	
RCA048	En los componentes lectores provistos o no por la entidad/operador para la lectura del factor "algo que tiene" (TD/TC) vinculados o no a dispositivos móviles o computadores personales, deben satisfacerse los siguientes requerimientos:: a. El valor capturado por el lector, debe ser encriptado desde el lector mediante un algoritmo no menor a 3DES para componentes que permitan transacciones establecidas con criticidad de nivel 1 en los escenarios del punto 6.5. b. El lector debe encontrarse asociado de manera univoca a los siguientes tres elementos: (1) red de procesamiento, dispositivo móvil o computador personal, (2) el servicio provisto por la entidad/operador y el (3) cliente/comercio. c. El lector debe ser homologado por la entidad/operador para la provisión del servicio.	

6.7.3. Tabla de requisitos de Integridad y Registro.

Tabla de requisitos de Integridad y Registro		
Código de requisito	**Descripción de requisito**	**Alcance**
RIR001	Los datos de autenticación de las credenciales no deben ser almacenados en el dispositivo provisto por la entidad/operador ni conservados en el registro de actividad del mismo (Journal).	
RIR002	El registro de las actividades en los sistemas aplicativos y/o dispositivos provistos por la entidad/operador, debe garantizar para cada evento al menos: a. Identificación. b. Descripción. c. Fecha y hora completa. d. Identificación de origen. e. Usuario actor.	
RIR003	Los registros colectados por los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quién (persona/dispositivo/cuenta/oriogen/destino), qué (actividad/función/transacción), dónde (CE, ubicación), cuándo (tiempo) y cómo (patrón/relación de eventos).	
RIR004	Los registros de los sistemas aplicativos y/o dispositivos provistos por la entidad/operador deben contemplar al menos los siguientes eventos: a. Solicitudes y respuestas a acciones transaccionales y de mantenimiento de las aplicaciones. b. Errores y fallas de la aplicación o el dispositivo. c. Intentos exitosos y fallidos de autenticación. d. Gestión de credenciales (alta, eliminación, modificación y asignación de privilegios). e. Gestión de bases de datos/repositorios (creación, eliminación, modificación y consultas). f. Acciones operativas y de mantenimiento (inicio y cierre de los sistemas, fallas y cambios en la configuración).	
RIR005	Los registros de las actividades de cada CE asociado al escenario deben contar desde el momento de su generación, con mecanismos que permitan verificar que cada registro sea único, responda a una secuencia predeterminada y se mantenga inalterable durante su almacenamiento, transporte y recuperación.	
RIR006	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben ser almacenados y custodiados mediante alguno de los siguientes regímenes de almacenamiento: a. En el caso de registros digitalizados (Electronic Journal) deben ser enviados en tiempo real o permanecer almacenados por menos de 24 horas en el dispositivo provisto por la entidad/operador que los generó, cuando aplique, debiendo ser trasladados a ese término a una infraestructura de almacenamiento y custodia. b. En el caso de registros impresos (Tira Journal) deben ser enviados en forma inmediata posterior a cada evento de balanceo y carga del dispositivo provisto por la entidad/operador.	
RIR007	Los registros históricos de las actividades y de las operaciones transaccionales deben conservarse por un término no menor a 6 años. Los soportes de almacenamiento del archivo histórico no deben ser recuperables luego de su descarte.	
RIR008	Los soportes de almacenamiento de los registros de las actividades y de operaciones transaccionales en el dispositivo provisto por la entidad/operador no deben ser recuperables luego de los siguientes situaciones: a. 15 días posteriores al traslado confirmado a la infraestructura de custodia y recuperación. b. El descarte del soporte de almacenamiento en el dispositivo.	
RIR009	Los registros de las actividades de los dispositivos/aplicaciones provistos por la entidad/operador y de las operaciones transaccionales, deben contar con mecanismos de protección que aseguren que sólo podrán ser accedidos por aquellos que corresponda según la necesidad de uso/conocimiento.	

Tabla de requisitos de Integridad y Registro (continuación)

Código de requisito	Descripción de requisito	Alcance
RIR010	Los dispositivos y/o piezas de software provistas por la entidad/operador para el uso del CE, deben asegurar que satisfacen un ciclo de vida y de desarrollo de sistemas, basado en las siguientes etapas conceptuales: a. Análisis de requerimientos. b. Adquisición/fabricación/desarrollo. c. Prueba y homologación. d. Implementación. e. Operación y mantenimiento. f. Descarte y reemplazo. Asimismo, este ciclo, debe proveer los elementos de seguridad relacionados con, pero no limitados a: g. Requisitos funcionales de seguridad. h. Tipos y características de validación de los datos de entrada. i. Granularidad de las funciones y los registros. j. Niveles de acceso. k. Control de Cambios. l. Actualización y Parches.	
RIR011	Los procesos de homologación de dispositivos y/o piezas de software provistos por la entidad/operador para interactuar con el CE, deben garantizar la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/desarrollo e implementación.	
RIR012	Los procesos de homologación e implementación de piezas de software del CE en dispositivos del cliente bancario, deben realizarse utilizando una verificación formal antes de su habilitación. Asimismo, deben utilizarse métodos de instalación que prevengan la exposición de datos personales, financieros o de las credenciales del cliente.	
RIR013	Deben efectuarse los siguientes controles de integridad de los datos transmitidos: a. Identificación del receptor y cuenta destino. b. Credenciales y cuenta de origen. c. Identificación y composición del mensaje.	
RIR014	En la transmisión de datos de credenciales y transacciones, todo punto de conexión entre una red privada y una red pública debe contar con un Firewall en cada conexión a Internet y entre cualquier zona desmilitarizada y la zona de la red interna, incluida toda red inalámbrica. Aplica solamente a la infraestructura de la entidad/operador que gestiona el CE con redes basadas en TCP/IP.	
RIR015	Cuando el transporte de datos de credenciales y transacciones se realice mediante el empleo de redes públicas y/o parcialmente privadas en alguno de sus tramos, la entidad/operador debe incluir mecanismos de protección del vínculo y la sesión en los CE, incluyendo pero no limitándose a: a. Uso de protocolos seguros para la transmisión de datos (tales como TLS/SSL/IPSEC/SSH) en redes públicas (tales como 3G, 4G/LTE, GSM, GPRS, WIFI, Internet). b. Uso de métodos de protección del sitio bancario (Certificados digitales basado en infraestructura de clave pública). c. cifrado sólido en redes que utilicen protocolos basados en TCP/IP. Este requisito es únicamente aplicable a los canales TAS, POS y ATM y cuando utilicen redes públicas con protocolos basados en TCP/IP.	
RIR016	En todos los casos, los dispositivos/aplicaciones provistos por la entidad/operador, deben poder generar un comprobante de la transacción efectuada que resulte único y verificable contra los registros de actividad del canal. Incluye pero no se limita a la aplicación alternativa de alguna de las siguientes opciones: a. Papel impreso para dispositivos físicos provistos por la entidad/operador. Emitirse a demanda del cliente en caso que no requiera firma del cliente, obligatoriamente cuando requiera firma del cliente, b. Formato digital para dispositivos propios del cliente, recuperable por al menos 3 meses posteriores a la transacción. Adicionalmente, los datos de identificación de las credenciales del cliente deben limitarse a los estricta y mínimamente necesarios y no deben aparecer de forma completa en el comprobante.	

Tabla de requisitos de Integridad y Registro (continuación)

Código de requisito	Descripción de requisito	Alcance
RIR017	En los procesos de compatibilización de dispositivos y/o implementación de piezas de software en entornos controlados por el usuario, la entidad/operador debe definir e informar al cliente bancario, los requisitos de seguridad aplicables a los dispositivos propios del usuario, realizando las siguientes tareas: a. Informar los criterios de admisibilidad de los dispositivos del usuario, así como las limitaciones de hardware, software, conectividad y entorno para su uso en el CE. b. El CE debe prevenir el acceso a través de un dispositivo que no satisface los criterios de admisibilidad determinados. c. Detectar e informar al usuario las acciones necesarias para mantener habilitado el servicio desde el dispositivo.	
RIR018	Las credenciales basadas en TD/TC que fueran retenidas durante el uso de los dispositivos provistos por la entidad/operador, deben asegurar el cumplimiento de las siguientes acciones operativas: a. Posterior a su retención la entidad/comercio debe informar al emisor antes de transcurridas 24 horas y en el menor tiempo posible de acuerdo con los medios disponibles. b. La entidad/operador emisor debe resolver el incidente en un lapso no mayor a 48 horas. c. En los casos que el material retenido no sea legítimo debe conservarse bajo custodia con los recaudos necesarios para evitar su uso, como material de prueba para posterior investigación.	
RIR019	Las aplicaciones (piezas de software) empleadas para brindar servicios financieros en dispositivos móviles deben garantizar la vinculación única entre la “aplicación”, las credenciales del cliente y el dispositivo móvil, considerando pero no limitándose a las siguientes técnicas combinadas:: a. Asociación de identificador IMEI (International Mobile Station Equipment Identity, por su siglas en inglés) o código único de identificación del dispositivo. b. Semilla para encripción de datos y/o credenciales c. Valor aleatorio que identifica la relación del dispositivo con el servicio financiero. Las aplicaciones para dispositivos móviles deben alojarse en sitios cuyas condiciones de seguridad sean acordes con la política de la entidad financiera y estos ser informados al consumidor de servicios financieros de manera fehaciente.	

6.7.4. Tabla de requisitos de Monitoreo y Control.

Tabla de Requisitos de Monitoreo y Control		
Código de requisito	**Descripción de requisito**	**Alcance**
RMC001	La entidad/operador debe establecer un tiempo máximo de inactividad de la sesión en cada dispositivo/aplicativo provisto al cliente para el uso del CE. Este tiempo debe garantizar que la sesión no permanezca abierta de forma indefinida e incluir pero no limitarse a las siguientes acciones: a. Expiración de la sesión por tiempo establecido para cada canal según análisis de vulnerabilidades documentado. b. Expiración de la sesión en un tiempo no mayor en ningún caso a 30 minutos.	
RMC002	Los dispositivos provistos por la entidad/operador que presenten problemas de comunicación o fallas de funcionamiento total o parcial de los mecanismos de seguridad (Control de Acceso, Integridad y Registro), deben asegurar un monitoreo oportuno basado en alertas y registro de las acciones emprendidas para su inhabilitación/reparación según corresponda.	
RMC003	Debe realizarse el seguimiento sobre los CE de los cambios de configuración de seguridad y verificar los niveles de actualización de: sistemas operativos, bases de datos, vínculos de comunicación, herramientas que previenen y detectan la presencia de código malicioso, equipamiento de seguridad de red, controladores de tráfico y cualquier otra herramienta de seguridad. Deben incluir, sin limitarse a: a. Seguimiento de privilegios y derechos de acceso. b. Procesos de copia, resguardo y recuperación de información. c. Disponibilidad de los dispositivos del CE. d. Alarmas, alertas y problemas detectados por los sistemas de registro de eventos. Este requisito no incluye los dispositivos propios del cliente, ni los elementos de autenticación basados en el factor “algo que tiene” provistos por la entidad/operador.	
RMC004	Las entidades deben disponer de mecanismos de monitoreo transaccional en sus CE, que operen basados en características del perfil y patrón transaccional del cliente bancario, de forma que advierta y actúe oportunamente ante situaciones sospechosas en al menos uno de los siguientes modelos de acción: a. Preventivo. Detectando y disparando acciones de comunicación con el cliente por otras vías antes de confirmar operaciones. b. Reactivo. Detectando y disparando acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas. c. Asumido. Detectando y asumiendo la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas.	
RMC005	Las entidades deben implementar mecanismos de comunicación alternativa con sus clientes con objeto de asegurar vías de verificación variada ante la presencia de alarmas o alertas ocurridas por efecto del monitoreo transaccional implementado.	
RMC006	A partir de los registros colectados por los sistemas aplicativos de la entidad/operador asociados al escenario, se debe realizar una clasificación y determinación de los eventos de seguridad, una definición de los límites y umbrales de compromiso, niveles de comportamiento normal/inesperado y establecer las acciones de acuerdo con cada clasificación y limite determinado.	
RMC007	Los dispositivos provistos por la entidad/operador que interactúen con TD/TC deben contar con mecanismos de alerta en caso de olvido y retención de la TD/TC, con excepción del canal POS.	
RMC008	La entidad financiera debe proveer vías de comunicación para la recepción de consultas/denuncias de los clientes las 24 horas.	

Tabla de requisitos de Monitoreo y Control (continuación)

Código de requisito	Descripción de requisito	Alcance
RMC009	Los sistemas de monitoreo transaccional de las entidades/operadores de TD/TC, deben asegurar la detección, registro y control de situaciones que establezcan un compromiso de datos sensibles que incluya pero no se limite a las siguientes: a. Punto común de compromiso. punto de venta, adquirente, proveedor, entre otros que comprometan transacciones de TD/TC cursadas por el mismo. b. Fuga de información. Pérdida ocurrida en la infraestructura técnica y/o organizacional de la entidad financiera, operador, adquirente, distribuidor y/o proveedores que comprometa información sensible de las TD/TC (números de tarjeta, códigos de seguridad, datos confidenciales del cliente, entre otros) c. Códigos de Seguridad. Compromiso demostrado de los algoritmos de cálculo de los códigos de seguridad de las TD/TC.	
RMC010	Los dispositivos/aplicaciones provistos por la entidad/operador, deben detectar la apertura simultánea de más de una sesión, para un mismo usuario, canal y entidad financiera, ejecutando una de las siguientes acciones: a. Impedir la apertura simultánea de más de una sesión b. Bloquear la operatoria inmediatamente después de la detección, informando al cliente de la irregularidad. El CE ATM podrá exceptuarse de las acciones indicadas en los puntos a y b siempre que se incluyan en los sistemas de monitoreo y control las configuraciones necesarias para detectar y registrar los eventos indicados en el requisito.	
RMC011	El monitoreo transaccional en los CE debe basarse, pero no limitarse a lo siguiente: a. La clasificación de ordenantes y receptores en base a características de su cuenta y transacciones habituales, incluyendo pero no limitándose a frecuencia de transacciones por tipo, monto de transacciones y saldos habituales de cuentas. b. Determinación de umbrales, patrones y alertas dinámicas en base al comportamiento transaccional de ordenantes y receptores según su clasificación.	
RMC012	El proceso de apertura de los dispositivos para ATM y TAS debe garantizar: a. Ser realizada por dos personas, dejando constancia escrita en un acta de su participación y del resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, entre otros. b. En los casos de dispositivos neutrales, la documentación de respaldo (planillas o formularios de balanceo, de reposición, de tarjetas retenidas, de conciliación y otras) debe ser firmada, posteriormente, por un funcionario de la entidad financiera, que será la figura responsable para cualquier intervención posterior ante requerimientos de este Banco Central.	
RMC013	Durante los procesos de mantenimiento, configuración, apertura, carga y balanceo de los dispositivos contemplados en el escenario, con excepción del canal POS, se deben satisfacer las siguientes consignas: a. Debe asegurarse una segregación física y lógica de las siguientes funciones: • Administración (instalación, configuración y ajuste de parámetros en el sistema operativo y aplicativo). Debe encontrarse limitada a personal del operador/entidad responsable del servicio. • Operación (ejecución de tareas operativas de consulta, balanceo y reporte). Debe limitarse a responsables de la entidad o tercero contratado por la entidad para los procesos indicados. • Apertura y cierre de dispositivo y tesoro. Debe aplicarse un control dual para el uso y posesión temporal de las llaves físicas y/o lógicas asegurando que en el proceso participan al menos dos personas donde preferentemente una de ellas debe pertenecer a la entidad. b. Debe asegurarse la puesta en práctica de procedimientos internos de la entidad para el control de la documentación de respaldo de las tareas operativas relacionadas.	

6.7.5. Tabla de requisitos de Gestión de Incidentes.

Tabla de requisitos de Gestión de Incidentes		
Código de requisito	**Descripción de requisito**	**Alcance**
RGI001	Debe realizar con una periodicidad mínima anual y con base en el análisis de riesgo de los activos informáticos asociados al escenario, un análisis de los incidentes ocurridos y un reporte que sirva para establecer medidas de protección, contenidos del programa de capacitación y concientización, modificaciones a la registración y control de eventos, y una redefinición de las alertas, límites y umbrales.	
RGI002	La identificación de incidentes debe estar basada al menos en alertas tempranas, estadísticas de tipo/frecuencia/patrón de incidentes y recomendaciones de seguridad informática.	
RGI003	La gestión de incidentes de seguridad puede ejecutarse en forma descentralizada pero debe ser coordinada con personal de la entidad financiera.	
RGI004	No definido.	
RGI005	Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.	

7.1. Actividades factibles de delegación.

Las entidades financieras podrán delegar en terceros actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, en las condiciones fijadas por la Comunicación CREFI – 2 en su Capítulo II, Sección 6, o posteriores modificaciones.

Las condiciones normativas y reguladoras serán exigibles y aplicables de igual forma cuando las actividades se realicen en dependencias de terceros.

No podrán delegarse actividades con proveedores que a su vez tengan contratada la función de auditoría interna y/o externa de las mismas.

7.2. Responsabilidades propias de la entidad.

El Directorio, o autoridad equivalente de la entidad financiera, debe establecer y aprobar formalmente políticas basadas en un previo análisis de riesgos, con el fin de gestionar eficientemente el proceso de delegación de actividades que le son propias, vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas.

La delegación de las actividades antes mencionadas, nunca debe entenderse como transferencia de las responsabilidades primarias enunciadas en la presente normativa.

Las políticas deben reconocer el nivel de riesgo al que se expone la entidad financiera en las relaciones de delegación de actividades en terceros. Las mismas deben ser apropiadas al tamaño y complejidad de las actividades delegadas.

Para toda actividad vinculada a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deberá evidenciarse la existencia de contratos que definan claramente el alcance de los servicios, las responsabilidades y acuerdos sobre confidencialidad y no divulgación.

En los casos de entidades que cuenten con servicios de tecnología delegados a terceras partes, el control de la gestión de las facilidades para la protección de activos de información debe ser realizado con recursos propios, ya sea en locación de la entidad o en locación del tercero.

7.3. Formalización de la delegación.

Los contratos deben fijar como mínimo: el alcance de las actividades; los niveles mínimos de prestación de servicios y su tipo; la participación de subcontratistas; los derechos a realizar auditorías por parte de la entidad; compromisos de confidencialidad; los mecanismos de resolución de disputas; la duración del contrato; cláusulas de terminación del contrato; los mecanismos de notificación de cambios en el control accionario y en los cambios de niveles gerenciales; el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera su-

frir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad de procesamiento.

Además, los contratos deben establecer claramente la inexistencia de limitaciones para la Superintendencia de Entidades Financieras y Cambiarias, en cuanto a: el acceso a los datos, la revisión y tenencia de toda documentación técnica relacionada (diseño de archivos, tipo de organización, etc.) y a la realización de auditorías periódicas en las instalaciones del proveedor, a fin de verificar el cumplimiento de todos los aspectos contemplados en estas normas.

7.4. Responsabilidades del tercero.

Los terceros, en los cuales se hayan delegado actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deben mantener la aplicación de las pautas mínimas establecidas en las presentes normas.

7.5. Implementación del procesamiento de datos en un tercero.

La delegación de las actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deben evidenciar una clara separación de actividades, en aquellos casos en que el tercero brinde servicios a múltiples organizaciones, ya sean entidades financieras o de otro tipo de negocio.

La gestión y la guarda de los datos de una entidad financiera evidenciarán una separación lógica y/o física de los datos de otra organización.

Los sistemas de administración de la seguridad de los datos, y de los programas relativos a una entidad financiera, tendrán un entorno de seguridad individual que pueda ser controlado y monitoreado exclusivamente por los responsables indicados por la propia entidad financiera.

7.6. Control de las actividades delegadas.

El Directorio, o autoridad equivalente de la entidad, es el responsable primario sobre el control y monitoreo continuo del cumplimiento de los niveles de servicios acordados, el mantenimiento de confidencialidad de la información y de todos los aspectos normados por la presente comunicación para las actividades que hayan sido delegadas.

El control y monitoreo deberán mostrar una continuidad en su ejecución, relacionada con el nivel de riesgos que la entidad haya analizado y asumido. Deberán existir planes de ejecución de controles y documentación formalizada de los mismos, como así también de los requerimientos de mejoras solicitados al tercero, en caso de incumplimientos.

7.7. Planificación de continuidad de la operatoria delegada.

El Directorio, o autoridad equivalente de la entidad, es el responsable primario en establecer la existencia de un plan de continuidad de las actividades delegadas en terceros, a los fines de no cesar con las actividades normales de la entidad financiera y asegurar la continuidad de los servicios ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios.

Asimismo, el Directorio, o autoridad equivalente de la entidad, es responsable de asegurar que el proveedor de servicios cuente con un adecuado plan de recuperación del procesamiento de datos, acorde a los requerimientos de negocio de la entidad y los niveles de riesgo asumidos por la misma. Este plan deberá ser probado en forma integral con frecuencia anual, la gerencia de la entidad deberá asegurar su resultado satisfactorio, y mantener documentación formal de las pruebas realizadas.

8.1. Cumplimiento de requisitos normativos.

Las entidades financieras deben considerar, en el diseño de los sistemas aplicativos que procesan su información comercial y de gestión, la implementación de apropiados controles según los requerimientos legales y reguladores vigentes, establecidos en las distintas comunicaciones emitidas por el Banco Central de la República Argentina.

Los requisitos mínimos de gestión, implementación y control de tecnología informática para los sistemas de información que se detallan en los siguientes puntos son aplicables a todas las entidades financieras, independientemente del tamaño, estructura, volumen y naturaleza de sus procesos de negocios. Asimismo, no son excluyentes de todos aquellos mecanismos adicionales que las entidades consideren que deben formar parte de su estrategia de administración y control informático.

8.2. Integridad y validez de la información.

En los sistemas aplicativos de información se deben implementar controles automatizados que permitan minimizar errores en la entrada de datos, en su procesamiento y consolidación, en la ejecución de los procesos de actualización de archivos y bases, y en la salida de la información.

Los datos que se registren en los sistemas deben ser sometidos a controles programados que aseguren la integridad, validez, confiabilidad y razonabilidad de la información procesada, incluyendo: dígitos verificadores, validaciones de códigos, tipo y tamaño de campos, rangos de valores, signos, referencias cruzadas, registro de operaciones fecha-valor, correlatividad de las operaciones, plazos, cierres y reaperturas de períodos, entre otros.

Se deben contemplar controles programados que limiten la modificación y la eliminación de datos -básicos y pactados- de las operaciones concretadas, movimientos y saldos. Asimismo, se deben implementar procesos automáticos para el devengamiento de intereses, el cálculo de cuotas, el redondeo de las cifras, y la aplicación de movimientos.

Debe existir una adecuada integración entre los sistemas aplicativos que procesan la información de la entidad y el sistema aplicativo de contabilidad. Se registrarán automáticamente en cada cuenta contable, en forma correcta y oportuna, todos los movimientos producto de las operaciones efectuadas.

En el sistema que administre la información sobre los clientes, se deben implementar adecuados controles de integridad, validez y razonabilidad, considerando la identificación única del cliente y los datos obligatorios de acuerdo con las normas vigentes. Además, deberán realizarse procesos periódicos de control y depuración sobre los mismos.

Los parámetros que limiten el ingreso de datos deben tener adecuados niveles de acceso para su actualización, y restricciones en cuanto a la posibilidad de ser modificados a través de funciones específicas.

Todos los sistemas aplicativos deben generar registros de auditoría que contengan mínimamente las actividades de los usuarios, las tareas realizadas, las funciones monetarias y no monetarias utilizadas, y quién ingresó y autorizó cada transacción, salvo que las mismas consistan en consultas o actividades, tareas o funciones similares que no generen transacciones o modificaciones en los datos o aplicativos. Estos registros deben ser revisados regularmente por los responsables del control. Se debe proteger la integridad de la información registrada en dichos reportes, la que debe ser resguardada adecuadamente y permanecer en condiciones de ser recuperada por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dichos registros podrá ser inferior a 6 (seis) años. La información podrá ser resguardada en soportes de almacenamiento no modificables o en soportes reutilizables, siempre que se proteja la integridad de la información con medidas de control que permitan evidenciar la no alteración posterior a su generación. Dichos registros deberán estar disponibles en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias los requieran para su control.

8.3. Administración y registro de las operaciones.

Las entidades financieras deben registrar y procesar sus operaciones en los sistemas aplicativos de información correspondientes. No deberá gestionarse ninguna operación en forma manual, en hojas de cálculo, herramientas de escritorio u otro software utilitario.

8.4. Sistemas de información que generan el régimen informativo a remitir y/o a disposición del Banco Central de la República Argentina.

Las entidades financieras deben contar con sistemas aplicativos o procesos automatizados para la generación de los regímenes informativos requeridos por el Banco Central de la República Argentina. Se deberá evitar el reingreso o intercambio no automatizado de datos entre distintos sistemas, el ingreso de datos significativos en forma manual, y no se podrán efectuar ajustes a la información generada previamente en forma automática.

En los casos en que se deba ingresar información manual por no residir ésta en los archivos o bases de datos de la entidad, se debe realizar a través de programas específicos, en archivos independientes, con un adecuado esquema de seguridad, controles de integridad y validez, y sin la posibilidad de modificar la información generada en forma automatizada.

La información generada debe ser sometida a procesos de control, que analicen la consistencia e integridad de la información a remitir y/o mantener a disposición del Banco Central de la Republica Argentina, y que en ningún caso permitan su modificación fuera de los sistemas aplicativos que la originaron.

8.5. Documentación de los sistemas de información.

8.5.1. Estándares para el proceso de ingeniería del software.

De acuerdo con la estructura y complejidad de sus funciones informáticas, las entidades financieras deben contar con estándares de metodología para el proceso de ingeniería del software, que comprendan aspectos tales como: estudio de factibilidad, análisis y especificaciones, diseño, desarrollo, pruebas, migraciones de datos preexistentes, implementación y mantenimiento de los sistemas aplicativos de información.

Los mismos deben ser tenidos en consideración, tanto para desarrollos de sistemas propios de la entidad, como para aquellos que hayan sido tercerizados a través de la contratación de personal o proveedores externos.

Asimismo, deben contar con procedimientos que definan el circuito para el tratamiento de los requerimientos de usuarios y pautas para la evaluación, selección y adquisición de sistemas aplicativos.

8.5.2. Documentación técnica y manuales de usuarios.

Las entidades financieras deben contar con documentación funcional y técnica actualizada de sus sistemas aplicativos de información, en la cual se deben considerar aspectos tales como: objetivo, alcance, diagrama del sistema y de los programas componentes de los mismos, diseño de archivos y bases de datos, registro de modificaciones, lenguaje de programación utilizado, propiedad de los programas fuentes, descripción del "hardware" y "software", su interrelación con las redes de telecomunicaciones y descripción de las funciones que permitan la modificación directa de datos de producción (cambio de parámetros, fórmulas, tasas, datos y otros).

Además, deben poseer manuales de usuarios finales de cada sistema aplicativo de información que contengan, por ejemplo: objetivo, alcance, descripción de las funciones y menús, descripción de los listados operativos y de control, e instrucciones para el caso de cancelaciones, entre otros.

B.C.R.A.	ORIGEN DE LAS DISPOSICIONES CONTENIDAS EN LAS NORMAS SOBRE "REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS"

TEXTO ORDENADO			NORMA DE ORIGEN				Observaciones
Sección	Punto	Párrafo	Com.	Anexo	Punto	Párrafo	
1.		1° a 3°	"A" 4609	único	1.	1° a 3°	
		4°	"A" 3198		1.	1°	
	1.1.		"A"4609	único	1.1.		
	1.2.		"A" 3198		1.2.		
	1.3.		"A" 3198		1.3.		
	1.4.		"A" 3198		1.4.		
	1.5.		"A"4609	único	1.5.		
	1.6.		"A" 3198		1.6.		
	1.7.		"A" 3198		1.7.		
		12° y 13°	"A" 3198			9° y 10°	
2.	2.1.		"A" 3198		2.5.		Según Com. "A" 4609.
	2.2.		"A" 3198		3.1. a 3.3.		Según Com. "A" 4609.
	2.3.		"A" 4609	único	2.3.		
	2.4.		"A" 3198		2.1. y 2.5.		Según Com. "A" 4609.
	2.5.1.		"A" 3198		2.3.		Según Com. "A" 4609.
	2.5.2.		"A" 3198		2.4.		
	2.5.3.		"A" 3198		2.2.		Según Com. "A" 4609.
	2.5.4.		"A" 4609	único	2.5.4.		
	2.5.5.		"A" 4609	único	2.5.5.		
3.	3.1.		"A" 4609	único	3.1.		
	3.1.1.		"A" 3198		6.1.		Según Com. "A" 4609.
	3.1.2.		"A" 4609	único	3.1.2.		
	3.1.3.		"A" 4609	único	3.1.3.		
	3.1.4.		"A" 3198		6.3. a 6.5.		Según Com. "A" 4609 y "A" 4690, pto. 1.
	3.1.5.		"A" 4609	único	3.1.5.		
	3.2.		"A" 4609	único	3.2.		
	3.2.1.		"A" 4609	único	3.2.1.		
	3.2.2.		"A" 3198		7.3.		Según Com. "A" 4609.
	3.2.3.		"A" 3198		7.3.		Según Com. "A" 4609.
	3.2.4.		"A" 4609	único	3.2.4.		
4.	4.1.		"A" 4609	único	4.1.		
	4.2.		"A" 4609	único	4.2.		
	4.3.		"A" 3198		7.2.		Según Com. "A" 4609.
	4.4.		"A" 3198		7.2.		Según Com. "A" 4609.
	4.5.		"A" 3198		7.2.		Según Com. "A" 4609.
	4.6.		"A" 3198		7.2.		Según Com. "A" 4609.
5.	5.1.		"A" 3198		4.2.3.		Según Com. "A" 4609.
	5.2.		"A" 4609	único	5.2.		
	5.3.		"A" 3198		4.1.		Según Com. "A"4609.

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS

TEXTO ORDENADO			NORMA DE ORIGEN				Observaciones
Sección	Punto	Párrafo	Com.	Anexo	Punto	Párrafo	
5.	5.4.		"A" 3198		7.1.		Según Com. "A" 4609.
	5.5.		"A" 4609	único	5.5.		
	5.6.		"A" 4609	único	5.6.		
	5.7.		"A" 4609	único	5.7.		
	5.8.		"A" 3198		4.2.1., 6.6. y 6.7.		Según Com. "A" 4609.
	5.9.		"A" 4609	único	5.9.		
	5.10.		"A" 4609	único	5.10.		
	5.11.		"A" 4609	único	5.11.		
	5.12.		"A" 4609	único	5.12.		
6.	6.1.		"A" 4609	único			Según Com. "A" 5374 y 6017.
	6.2.		"A" 3198				Según Com. "A" 4609, 4690, 5374 y 6017.
	6.3.		"A" 4609	único			Según Com. "A" 4690, 5374 y 6017.
	6.4.		"A" 4609	único			Según Com. "A" 4690, 5374 y 6017.
	6.5.		"A" 4609	único			Según Com. "A" 5374 y 6017.
	6.6.		"A" 3198				Según Com. "A" 5374 y 6017.
	6.7.		"A" 4609	único			Según Com. "A" 5374 y 6017.
7.	7.1.		"A" 4609	único	7.1.		
	7.2.		"A" 4609	único	7.2.		
	7.3.		"A" 3198		5.1.		Según Com. "A" 4609.
	7.4.		"A" 3198		5.2. a 5.4.		Según Com. "A" 4609.
	7.5.		"A" 3198		5.5.		Según Com. "A" 4609.
	7.6.		"A" 3198		5.4.		Según Com. "A" 4609.
	7.7.		"A" 3198		5.6.		Según Com. "A" 4609.
8.	8.1.		"A" 3198		9.2.		Según Com. "A" 4609.
	8.2.		"A" 3198		4.2.2.		Según Com. "A" 4609 y 4690 (pto. 6.).
	8.3.		"A" 4609	único	8.3.		
	8.4.		"A" 3198		9.4.		Según Com. "A" 4609.
	8.5.1.		"A" 4609	único	9.1.		
	8.5.2.		"A" 3198		9.1.		Según Com. "A" 4609.

Comunicaciones que componen el historial de la norma

Últimas modificaciones efectuadas:

19/07/07: “A” 4690

12/12/12: “A” 5374

15/07/16: “A” 6017

Últimas versiones de la norma - Actualización hasta:

11/12/12

14/07/16

Texto Base:

Comunicación "A" 4609: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.

Comunicaciones que dieron origen y/o actualizaron esta norma:

"A" 4690: Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con Tecnología Informática y Sistemas de Información. Modificaciones.

“A” 5374: Circular RUNOR 1 - 1005. Normas sobre "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras". Modificación.

“A” 6017: “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”. Modificaciones.

“B” 9042: Comunicaciones “A” 4690 y “C” 48583. Actualización de texto ordenado.

“C” 48583: Fe de erratas Comunicación “A” 4609.

“C” 72331: Comunicación “A” 6017. Fe de erratas.